Dell™ Digital Forensics

Guida della soluzione

Messaggi di N.B., Attenzione e Avvertenza

N.B.: una NOTA evidenzia informazioni importanti per l'uso ottimale del computer.

ATTENZIONE: un messaggio di ATTENZIONE indica la possibilità che si verifichi un danno all'hardware o una perdita di dati se non vengono seguite le istruzioni.

AVVERTENZA: un messaggio di AVVERTENZA indica un potenziale rischio di danni materiali, lesioni personali o morte.

Le informazioni contenute nel presente documento sono soggette a modifiche senza preavviso.
© 2011 Dell Inc. Tutti i diritti riservati.

È severamente vietata la riproduzione di questi materiali, con qualsiasi strumento, senza l'autorizzazione scritta di Dell Inc.

Marchi commerciali utilizzati in questo documento: Dell™, il logo DELL™, PowerEdge™, EqualLogic™ e PowerConnect™ sono marchi commerciali di Dell Inc. Oracle® è un marchio commerciale registrato di Oracle Corporation e/o dei suoi affiliati. Citrix®è un marchio commerciale registrato di Citrix Systems, Inc. negli Stati Uniti e/o altri paesi.

Altri marchi e nomi commerciali possono essere utilizzati nel presente documento sia in riferimento alle aziende che rivendicano i marchi e i nomi che ai prodotti stessi. Dell declina ogni responsabilità in relazione ad interessi proprietari di marchi e nomi depositati diversi da quelli di sua proprietà.

2011 - 07 **Rev. A00**

Sommario

1 Introduzione 7

Ciclo di vita di Dell Digital Forensics **9**

La soluzione Dell facilita la gestione delle problematiche del settore **11**

Componenti della soluzione **12**

Sul campo. 12

Nel datacenter 13

Informazioni su questo documento **16**

Documentazione e risorse correlate **16**

2 Valutazione 17

Cos'è il processo di Valutazione? **17**

Vantaggio della soluzione Valutazione di Dell **17**

Raccolta di prove digitali di ambito forense **19**

Acquisizione standard vs. Acquisizione Live **20**

Come eseguire il software Valutazione con la soluzione Dell Digital Forensics **20**
Accendere il portatile Dell rugged 20
Masterizzare un CD di avvio per le procedure di acquisizione standard 21
Registrare un collector o un disco archivio 21
Pulire un collector o un disco archivio 23
Configurare un profilo collector 23
Utilizzare strumenti di valutazione 33
Revisione dei file raccolti dopo la valutazione . . . 36

3 Ingerisci 39

EnCase 6 abilitato per datacenter **39**
Soluzione singolo server 40
Soluzione multi-server (High Availability) 40

FTK 1.8 abilitato per datacenter **42**
Sessione FTK 1.8 singola per desktop 42
Sessioni FTK 1.8 multiple per desktop 42

FTK 3 abilitato per datacenter **43**
Soluzione server FTK 3 singola 44
Soluzione multiserver (no High Availability) 44

FTK 3, Lab Edition **46**

Molteplici applicazioni Forensics fornite in un desktop **47**

Consigli sulla configurazione di rete **48**

Come eseguire l'ingestione con la soluzione Dell Digital Forensics **51**
Ingerisci con SPEKTOR 51
Ingerisci con EnCase 53
Ingerisci con FTK 1.8 e 3.0 abilitato per datacenter . . . 56
Ingerisci con FTK 3 Lab Edition 59

4 Memorizza 61

Efficienza **61**

Scalabilità **62**

Protezione **62**

Livello di accesso fisico 62

Livello di controllo amministrativo e Active Directory 63

Livello di protezione basato su computer e Active Directory 64

Storage multi-tier **64**

Corrispondenza dell'archiviazione e del ripristino delle prove con il caso reale **65**

Come impostare Storage Security utilizzando la soluzione Dell Digital Forensics e Active Directory. . . . **66**

Creazione e popolamento di gruppi in Active Directory 66

Applicazione di policy di protezione utilizzando i GPO 67

Creazione e modifica di GPO 67

Modifica di un nuovo GPO (Windows Server 2008) 68

Supporto Active Directory per le policy di password sicura 68

Account utente Active Directory 69

Creare un account utente non amministrativo . . . 71

Configurazione protezione per file di casi individuali e riguardanti le prove 72

5 Analizza 73

Tipi di analisi **73**
Analisi hash 73
Analisi firma file 74

Cos'è l'elaborazione distribuita? **75**

Utilizzo di elaborazione distribuita in FTK 3.1 . . . . . **75**
Verifica installazione 77

Identificazione file su rete **77**

Analisi con FTK **78**
Aprire un caso esistente 78
Elaborazione prove di un caso 78

Analisi con EnCase **78**
Aprire un caso esistente 78
Creare un lavoro di analisi 79
Eseguire un lavoro di analisi 79
Esecuzione dell'analisi della firma 80
Visualizzazione dei risultati dell'analisi della firma 80

6 Presenta 81

Come creare report con la soluzione Dell Digital Forensics **81**
Creare ed esportare report con EnCase 6 81
Report con FTK 82

7 Archivia 83

Soluzione di archiviazione con un singolo clic del client **84**

Consigli per il backup Dell **85**

Backup di prove e file dei casi 85

Altro host vs. Rete 86

Come creare report con la soluzione Dell Digital Forensics **89**

Archiviazione on demand. 89

Requisiti. 89

Installazione 89

Archivia: con ODDM del software NTP 89

8 Risoluzione dei problemi 91

Suggerimento sulla risoluzione dei problemi. **91**

Problematiche specifiche del software Forensics . . . **91**

EnCase: EnCase si avvia in modalità Acquisizione 91

FTK Lab: il browser avviato dal client non riesce a visualizzare l'Interfaccia Utente 92

FTK 1.8: messaggio di limite\versione di prova 5000 oggetti 92

FTK 1.8: impossibile accedere, l'errore Access Temp File viene visualizzato all'avvio. 92

Problematiche Citrix. **92**

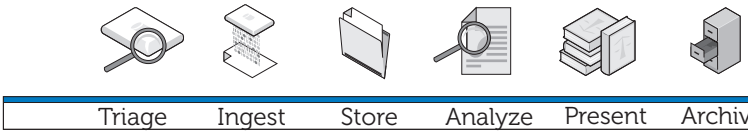
Le applicazioni Citrix: non si avviano 92

Applicazioni Citrix bloccate o arrestate 93

Indice analitico 95

1

Introduzione



Negli ultimi anni si è verificato un aumento esponenziale del volume, della velocità, della varietà e della sofisticazione delle attività digitali da parte di criminali e gruppi terroristici in tutto il mondo. Oggi la maggior parte dei crimini ha uno componente digitale. Qualcuno ha definito questo contesto come una *tsunami digitale*. Questa crescita è stata promossa anche dagli incredibili progressi dell'hardware elettronico. La diversità imperversante dei dispositivi elettronici di consumo e la loro capacità di memoria e storage in aumento offrono a criminali e terroristi una ricchezza di opportunità per nascondere le informazioni dannose.

Non è raro per PC e computer portatili possedere dischi rigidi dell'ordine di centinaia di gigabyte di storage. Gli ultimi dischi rigidi includono opzioni per uno o quattro megabyte. Considerate che un singolo terabyte è in grado di memorizzare il contenuto di 200 DVD: una grande quantità di memoria che rappresenta un problema che continuerà solo a crescere.

Dai PC ai computer portatili, dai telefoni cellulari alle chiavette USB e persino le console per videogiochi, i professionisti della scientifica digitale vengono spinti al limite per clonare, ingerire, indicizzare, analizzare e memorizzare quantità crescenti di dati sospetti, preservando allo steso tempo la catena digitale di custodia e continuando a proteggere i cittadini.

Tabella 1-1. Quanto grande è uno zettabyte?

Kilobyte (KB)	1.000 byte	2 KB	una pagina scritta
Megabyte (MB)	1.000.000 byte	5 MB	i lavori completi di Shakespeare
Gigabyte (GB)	1.000.000.000 byte	20 GB	una buona collezione di opere di Beethoven
Terabyte (TB)	1.000.000.000.000 byte	10 TB	una libreria di ricerca accademica
Petabyte (PB)	1.000.000.000.000.000 byte	20 PB	produzione di unità disco rigido annuale
Exabyte (EB)	1.000.000.000.000.000.000 byte	5 EB	tutte le parole possibile pronunciate dagli esseri umani
Zettabyte (ZB)	1.000.000.000.000.000.000.000 byte	2 ZB	dati creati globalmente durante il 2010 attesi*

* Roger E. Bohn, et. al., How Much Information? 2009, Global Information Industry Center, University of California, San Diego (gennaio, 2010).

Quando i presunti criminali vengono accusati e i computer e tutte le altre risorse digitali sequestrate, i professionisti della scientifica digitale ricevono un'enorme pressione per elaborare e analizzare le potenziali prove in brevissimo tempo e in ambienti meno adatti a garantire le esigenze probatorie. E quando sono le intere organizzazioni ad essere sospettate di attività criminali o terroristiche, il numero di dispositivi da analizzare può degenerare in modo drammatico.

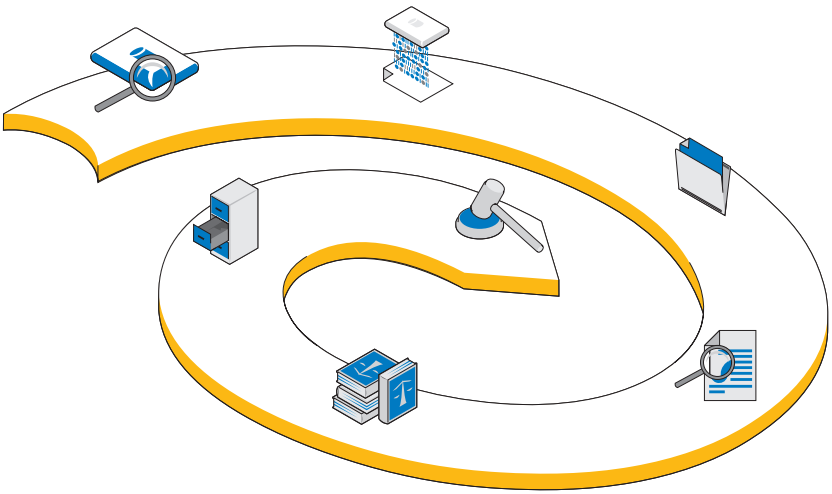
La scientifica digitale fornisce un mezzo per acquisire dati recuperati da computer o altri dispositivi digitali (cellulari, console di gioco, unità flash, GPS, ecc.), e l'esame scientifico e l'analisi di tali dati in modo da garantire che tali informazioni possano essere utilizzate in tribunale. La soluzione Dell Digital Forensics comprende la prima vera soluzione end-to-end a livello aziendale per forze dell'ordine, aziende e agenzie di sicurezza governative e organizzazioni e-discovery, fornendo l'insieme di hardware, software, servizi e supporto necessari per raccogliere, valutare, ingerire o creare imaging, memorizzare, analizzare, report e archiviare prove digitali.

Utilizzando il server aziendale scalabile e conveniente e l'hardware di storage di Dell, a seconda dei requisiti del proprio ambiente software, i sistemi di database Oracle sul back-end, una combinazione di computer portatili rugged e software SPEKTOR di Dell ed un servizio completo assieme al supporto Dell, il personale investigativo può condurre la valutazione dei dati della scientifica digitale e la raccolta di dati in modo rapido e semplice, garantendo la catena di custodia dal campo al datacenter e fino in aula.

Ciclo di vita di Dell Digital Forensics

La soluzione Dell Digital Forensics assiste a gli investigatori della scientifica nelle sei fasi del ciclo di vita dell'investigazione della scientifica: Triage (Valutazione), Ingest (Ingerisci), Store (Memorizza), Analyze (Analizza), Present (Presenta) a Archive (Archivia).

Figura 1-1. Ciclo di vita di Dell Digital Forensics



Valutazione

Il processo di valutazione permette all'investigatore digitale della scientifica di visualizzare rapidamente il contenuto di dispositivi di destinazione per determinare se il dispositivo deve essere rimosso e condotto nel laboratorio per ulteriori analisi e per la preparazione per la presentazione in tribunale.

Ingerisci

Ingerisci è la fase del processo della scientifica digitale in cui i dati obiettivo sono ripresi (a meno che non siano stati ripresi nel campo come parte della fase di valutazione), e una copia esatta del dispositivo di memorizzazione sospetto viene creata in modo tale che l'integrità del duplicato sia garantita confrontando gli hash di entrambi i dischi originali e duplicando i dati.

Nelle comuni pratiche esistenti, i dati sospetti *vengono ripresi* all'interno della soluzione Dell Digital Forensics. Invece di dati di immagini su una singola workstation, tuttavia, i dati ripresi vengono ingeriti in un repository centrale delle prove. Ingerendo dati immediatamente nel data center, i dati sono a disposizione di più analisti, il trasferimento da un dispositivo ad un altro è ridotto al minimo e la produttività e l'efficienza sono notevolmente migliorate. L'ingestione può, tuttavia, svolgersi sul campo se la capacità di archiviazione di destinazione è abbastanza ridotta. La soluzione Dell Digital Forensics offre l'ingestione sul sito tramite l'uso di un modulo SPEKTOR Imager opzionale.

Memorizza

La soluzione Dell Digital Forensics offre un'ampia gamma di possibili opzioni di accesso allo storage e alla rete per assecondare ogni singolo cliente. Storage e ripristino ad elevate velocità in ambienti di rete di livello enterprise permettono una configurazione multiutente che aumenta l'efficienza e la produttività. Gli analisti non dovranno più allocare le proprie risorse di elaborazione individuali per completare l'analisi delle prove, in quanto il tutto avviene su un server dedicato proprio a quello scopo.

Analizza

La capacità di elaborazione parallela offerta dalla soluzione Dell Digital Forensics permette all'analista di indicizzare a valutare i dati su server dalle elevate prestazioni anziché sui PC individuali. In aggiunta, è possibile eseguire sessioni con analisti contemporaneamente su workstation singole o multiple utilizzando le configurazioni back-end comprese dalla soluzione. Questa capacità aiuta a proteggere l'integrità del sistema e delle prove, aiuta a prevenire la necessità di creare la workstation se codici maligni vengono eseguiti per errore, aiuta a preservare la catena di custodia e ovvia al bisogno di ricreazione della workstation quando si passa da un caso all'altro. Nell'ambiente Digital Forensics, la *Catena di custodia* potrebbe essere definita come il mantenimento dell'integrità dei dati digitali come prove a partire dal momento in cui vengono raccolti fino al momento in cui vengono riportati e, infine, fino al momento in cui verranno presentati in aula.

Presenta

Utilizzando la soluzione Dell Digital Forensics, i team di visualizzazione e gli investigatori possono accedere alle potenziali prove di un caso in modo sicuro e in tempo reale, riducendo così il bisogno di rilasciare prove su DVD o richiedere agli esperti di dover raggiungere il laboratorio per motivi di accesso ai file.

Archivia

La soluzione Dell offre backup, ripristino e infrastrutture di archiviazione formalizzati per aiutare ad ottimizzare la cooperazione tra le agenzie e le divisioni di sicurezza anche oltre frontiera, a liberarsi dai costi amministrativi, a garantire la coerenza tra i laboratori e minimizzare i rischi per la catena di custodia digitale.

Inoltre, il modello della soluzione Dell Digital Forensics include un componente opzionale di ricerca che permette la correlazione di informazioni tra insiemi di dati ingeriti.

La soluzione Dell facilita la gestione delle problematiche del settore

Utilizzando la soluzione Dell Digital Forensics è possibile rendere il processo di portare prove digitali dalla scena del crimine al tribunale infinitamente più semplice per i professionisti investigativi, fornendo:

- Una rete di datacenter all'avanguardia che accelera l'ingestione, l'analisi e la condivisione di informazioni digitali
- Sicurezza delle informazioni con ulteriore automatizzazione del processo di indagine scientifica digitale, riducendo così il rischio di errore e compromissione dei dati
- Ulteriore sicurezza dell'integrità dei dati, attualmente attraverso l'utilizzo dei protocolli hash più sicuri, e presto attraverso l'implementazione di una funzione di controllo che consentirà di automatizzare i record della catena di custodia

N.B.: qualsiasi conclusione e raccomandazione contenuta nel presente documento che possa assomigliare ad un tipo di consulenza legale deve essere controllata tramite un consulente legale. Verificare sempre con la vostra giurisdizione locale, con i pubblici ministeri locali, e con il laboratorio della scientifica locale il metodo preferito di raccolta delle prove digitali.

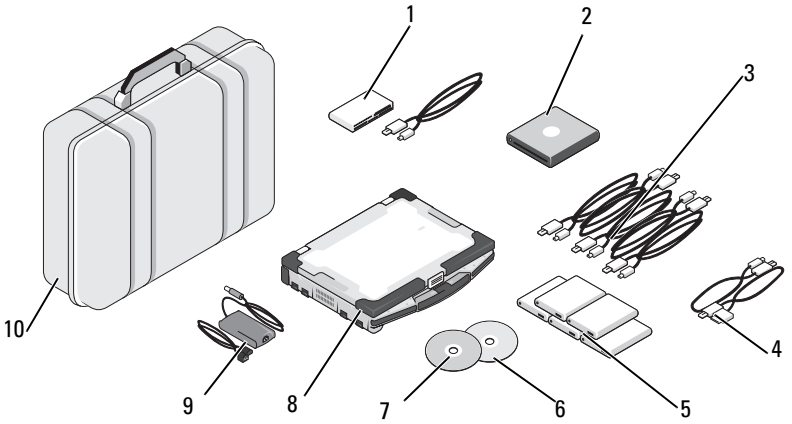
- Una soluzione end-to-end completa capace di ridurre in modo significativo la complessità di progettazione, realizzazione e gestione del processo di investigazione della scientifica digitale di livello enterprise
- Una soluzione conveniente e flessibile, modulare e scalabile, espandibile e con un piano tariffario prepagato

Componenti della soluzione

Sul campo

La porzione mobile della soluzione viene offerta in una custodia rigida progettata per entrare nello spazio del bagaglio a mano di un aereo. La custodia rugged contiene tutti gli strumenti e i software richiesti per la valutazione in sito di dispositivi di storage sospetti e include un portatile Dell E6400 XFR rugged con il software SPEKTOR Forensics preinstallato, Tableau Forensics Write-Blockers con accessori, un numero opzionale di dischi rigidi USB esterni con licenza per lavorare con il software SPEKTOR come *collector* di immagini di valutazione, un lettore schede 50:1 e gli adattatori e i cavi elencati in Figura 1-2.

Figura 1-2. Soluzione Dell Digital Forensics: componenti mobili



1	Lettore schede 50:1	6	Disco di ripristino immagine
2	DVD ROM USB	7	Disco di avvio SPEKTOR
3	Cavi USB del collector	8	Portatile Dell rugged
4	Cavi telefonici con opzione SPEKTOR PI (opzionali)	9	Alimentatore portatile Dell rugged
5	Collector del disco rigido esterno (5)	10	Custodia Pelican

Nel datacenter

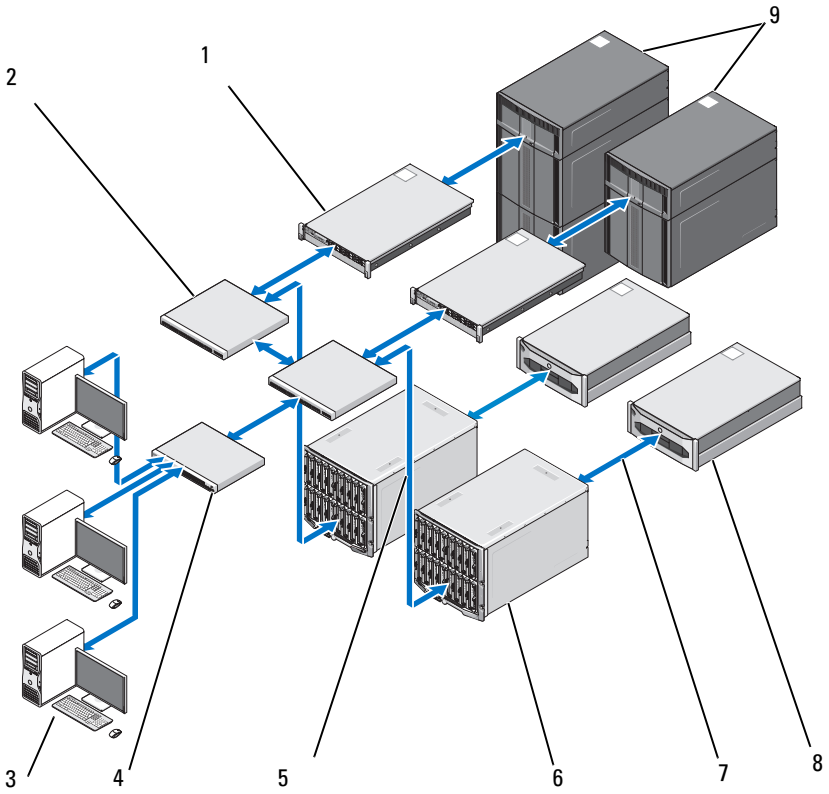
Nel datacenter, la soluzione Dell Digital Forensics include una configurazione personalizzata dei seguenti componenti:

- Server rack Dell PowerEdge R410, R610 e R710
- Server blade Dell PowerEdge M610 e M710
- SAN Dell EqualLogic 4000\6000 Series
- Windows Server 2008 R2
- Citrix XenApp 6.0
- AccessData FTK 1.8, AccessData FTK 3, AccessData Lab
- Guidance EnCase 6.15

- On-Demand Data Management (ODDM) del software NTP
- Symantec Enterprise Vault
- Symantec Backup Exec 2010
- Switch Dell PowerConnect
- Switch di rete Extreme

Il rack Dell PowerEdge e i server blade possono avere molteplici ruoli: server per file, server per prove, server per archivio, server per database, server di licenze EnCase e FTK, server per backup o controller del dominio. Supportano Microsoft Active Directory e tutte le policy di protezione e il software Forencics che compongono la soluzione Dell Digital Forensics.

Figura 1-3. Dell Digital Forensics Solution: datacenter



1	Server PowerEdge R410 o R610 (opzionale)	6	Server con blade Dell PowerEdge M1000E e M610
2	Switch Dell PowerConnect	7	Stream di dati da 10 GB
3	Workstation Dell Precision o OptiPlex	8	Sistemi di storage Dell EqualLogic PS4000 oe PS6000 series
4	Switch Dell PowerConnect	9	Storage di classe ML Dell PowerVault
5	Stream di dati da 1 GB		

Informazioni su questo documento

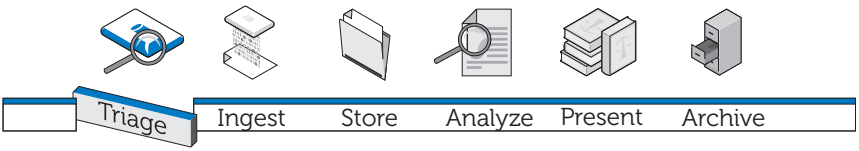
Questo documento copre ogni fase del processo digitale della scientifica in un capitolo dedicato, con capitoli aggiuntivi per la risoluzione dei problemi hardware e software supportati dalla soluzione. Ognuno dei capitoli inizia con una discussione sulle best practice e sulle problematiche specifiche che si possono incontrare quando si sceglie di implementare e gestire le soluzioni, quindi si sposta verso una descrizione generale sui vari strumenti e componenti rilevanti per quella fase della soluzione.

Documentazione e risorse correlate

È possibile accedere ad informazioni aggiuntive all'indirizzo **support.dell.com/manuals**.

2

Valutazione



Cos'è il processo di Valutazione?

L'opzione Valutazione permette all'investigatore della scientifica digitale di sfogliare i dati contenuti su dispositivi sospetti e di prendere decisioni su quali dispositivi sono in realtà probatori e per i quali vale la pena eseguire il sequestro per l'imaging già in loco (se i dati comprendono un piccolo volume) o per l'imaging da effettuare in seguito nel datacenter. Questa capacità di visualizzare in anteprima e catturare solo i dispositivi di destinazione può ridurre sostanzialmente i ritardi che influiscono sulla capacità degli investigatori di presentare le prove in modo tempestivo. La funzionalità di Valutazione può ridurre l'arretrato di dispositivi di storage in attesa di immagini presso il laboratorio della scientifica, utilizzando meno risorse, evitando l'aggiunta di una coda di ingestione già sovraccarica e riducendo drasticamente i costi operativi.

Vantaggio della soluzione Valutazione di Dell

Mobile

La soluzione Dell Digital Forensics può essere sulla scena del crimine con gli investigatori stessi; tutti i componenti sono stati accuratamente pre-testati per lavorare insieme, e coprono una vasta gamma di porte dei dispositivi di destinazione e connettori che ci si potrebbe aspettare di trovare sul campo.

Veloce

Le soluzioni esistenti per la valutazione possono rivelarsi lente e possono portare anche ala perdita dei dati perché svolgono compiti, come ad esempio ricerche per parole chiave o corrispondenza hash durante la raccolta dei dati. La soluzione Dell Digital Forensics supera questo ostacolo utilizzando la potenza di calcolo del portatile Dell rugged piuttosto che il PC di destinazione per eseguire analisi sui dati raccolti. In alcuni casi, potreste essere in grado di evitare del tutto i processi di imaging e indicizzazione in laboratorio.

Facile da utilizzare

I componenti della funzionalità Valutazione sono pronti all'uso giusto fuori dalla custodia rigida. Il software pre installato offre un'interfaccia intuitiva touch screen. Sono inoltre presenti profili definiti dall'utente e profili di raccolta riutilizzabili per i diversi scenari per l'utilizzo standard.

Accettabili in ambito forense

Il software di valutazione rafforza un processo efficiente e accettabile in ambito forense, assicurando che ogni tipo di prova potenziale venga raccolta, rivista e conservato senza compromessi.

Flessibile

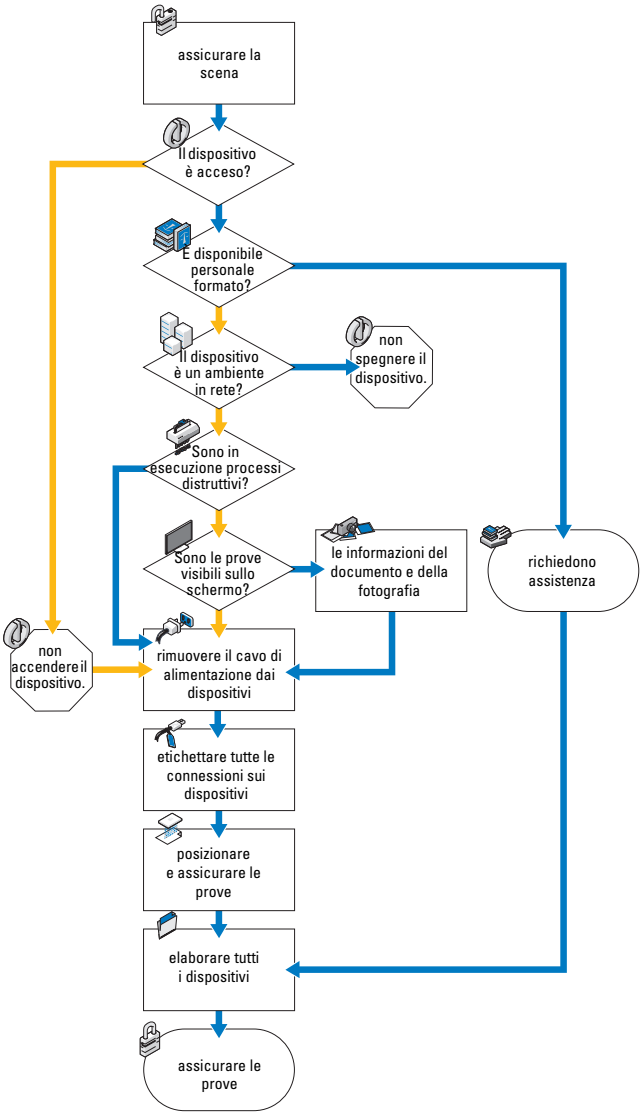
I componenti di Valutazione possono essere utilizzati per esaminare i dispositivi e le piattaforme di storage digitali più comuni, inclusi i dispositivi con sistema operativo Windows e Mac OS X di Apple, così come un'ampia gamma di tipi di dispositivi di storage digitali quali lettori MP3, dischi rigidi esterni, schede di memoria, telefoni cellulari e satellitari, unità GPS, iPad e iPhone e unità flash. Inoltre, i risultati ottenuti con il software Valutazione sono esportabili in altri programmi grazie all'utilizzo della soluzione Dell Digital Forensics.

Potente

Il portatile Dell rugged controlla l'intero processo, dall'esecuzione di un'analisi automatizzata dei dati di destinazione finale alla fornitura di risultati dettagliati in report dal formato di facile uso e in pochi minuti dopo l'acquisizione dei dati. Utilizzando la soluzione Dell, l'investigatore sarà in grado di eseguire scansioni di valutazione multiple in parallelo con una singola chiave di licenza.

Raccolta di prove digitali di ambito forense

Figura 2-1. Flusso della raccolta


assicurare la scena
Il dispositivo è acceso?
È disponibile personale formato?
Il dispositivo è un ambiente in rete?
non spegnere il dispositivo.
Sono in esecuzione processi distruttivi?
Sono le prove visibili sullo schermo?
le informazioni del documento e della fotografia
richiedono assistenza
non accendere il dispositivo.
rimuovere il cavo di alimentazione dai dispositivi
etichettare tutte le connessioni sui dispositivi
posizionare e assicurare le prove
elaborare tutti i dispositivi
assicurare le prove

Acquisizione standard vs. Acquisizione Live

La soluzione Dell Digital Forensics offre due tipi di acquisizione: un tipo standard e uno Live. Nel corso di una procedura di acquisizione standard, il computer portatile rugged Dell utilizza il disco di avvio di SPEKTOR per acquisire i dati di valutazione da un dispositivo di storage di destinazione già spento. Una procedura di valutazione con acquisizione Live invece, si propone di acquisire i dati di valutazione da un dispositivo di destinazione ancora alimentato, raccogliendo così prove non altrimenti disponibili.

In precedenza, gli standard di settore richiedevano che l'investigatore scollegasse e sequestrasse un dispositivo digitale per trasportarlo ed eseminarlo in laboratorio. Questa pratica implicava la perdita di elementi di prova potenzialmente preziosi sotto forma di accumulazione di dati volatili: tutti i dati memorizzati negli appunti, file aperti, il contenuto della RAM e le password memorizzate nella cache, ecc. Inoltre, i dati crittografati potrebbero andare persi nel caso il computer sia spento prima dell'imaging del disco. Inoltre, molti computer hanno password per il BIOS e per il disco rigido che sono determinate dall'utente e togliere l'alimentazione ad un sistema live con password del BIOS può causare la perdita di accesso all'intero contenuto del dispositivo.

Le best practice di settore richiedono al ricercatore di approcciare un dispositivo di archiviazione dati sospetto tenendo conto delle seguenti linee guida:

- Se il dispositivo è acceso, tenerlo acceso dove possibile fino a che venga eseguita un'approfondita indagine
- Se il dispositivo viene spento, lasciarlo spento

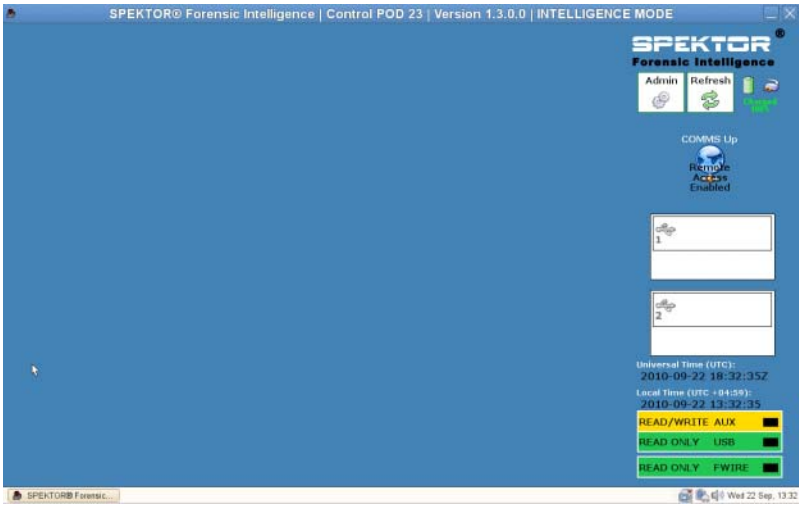
La ragione di queste linee guida è che il ricercatore deve essere attento a mantenere il dispositivo di archiviazione come lui lo trova sulla scena, e a determinare le minori modifiche possibili al dispositivo e al suo contenuto.

Come eseguire il software Valutazione con la soluzione Dell Digital Forensics

Accendere il portatile Dell rugged

1. Premere il pulsante di accensione per accedere al portatile Dell rugged. Il portatile carica automaticamente il software SPEKTOR.
2. Sfiorare o fare clic su **Accept EULA**. La schermata **Home** si apre.

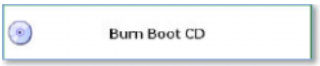
Figura 2-2. Schermata Home



Masterizzare un CD di avvio per le procedure di acquisizione standard

1 Nella schermata **Home**, sfiorare o fare clic su **Admin**. Quindi sfiorare o fare clic su **Burn Boot CD**.

Figura 2-3. Masterizzare un CD di avvio nella schermata Home



2 Seguire le istruzioni sulla schermata e quindi fare clic su **Finish**.

Registrare un collector o un disco archivio

N.B.: i collector devono essere concessi in licenza ed essere configurati da SPEKTOR prima di poter essere utilizzati con la soluzione Dell Digital Forensics. Contattare l'amministratore di sistema se si necessita di ulteriori collector o licenze.

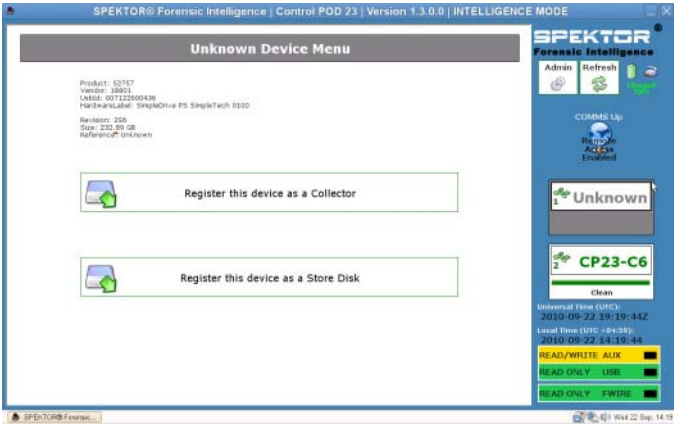
1 Collegare un nuovo collector o un nuovo disco archivio ad una delle porte USB sul lato sinistro del portatile Dell rugged. Il dispositivo viene visualizzato sullo schermo come un dispositivo sconosciuto.

Figura 2-4. Indicatore di collector sconosciuti o stato del disco archivio

2 Sfiorare o fare clic sull'icona **Status Indicator** che corrisponde al collector o al disco archivio collegato al portatile Dell rugged. L'icona del dispositivo che è stato registrato diventerà verde (per un collector) o arancione (per un disco archivio).

3 Verrà dunque visualizzato **Unknown Device Menu**.

Figura 2-5. Menu dispositivo sconosciuto



4 Sfiorare o fare clic su **Register this device as a Collector** o **Register this device as a Store Disk**.

5 Sfiorare o fare clic su **Yes**.

L'indicatore di stato mostra il nuovo numero di collector o di dischi archivio ed il suo stato diventerà **Dirty**.

Figura 2-6. Icone Dirty Collector e Store Disk

N.B.: i collector e i dischi archivio, sia che siano recentemente registrati sia che siano stai utilizzati per la raccolta di altri dati, devono essere puliti prima di potere essere utilizzati a confronto con un dispositivo di destinazione.

6 *For a store disk only*, inserire il numero seriale del disco archivio.

Pulire un collector o un disco archivio

N.B.: pianificate approssimativamente due ore per un volume del collector di 100 GB.

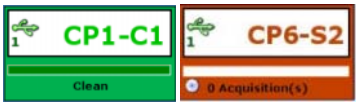
1 Selezionare lo **Status Indicator** che rappresenta il collector che si desidera pulire.

2 Nel **Collector Menu**, sfiorare o fare clic su **Clean Collector**.

3 Sfiorare o fare clic su **Yes** per confermare la selezione. La pulizia ha inizio e lo **Status Indicator** conferma il processo di pulizia.

Quando la pulizia viene completata, il software esegue un programma di verifica per confermare che i gli unici caratteri sull'unità collector siano zeri.

Figura 2-7. Indicatori di stato di collector e disco archivio registrato e pulito



N.B.: se il processo di pulizia non ha avuto successo, l'indicatore di stato indica che il collector resta sporco. È necessario reiniziare il processo di pulizia. Se la pulizia non viene completata con successo per una secondo volta, provare un altro collector o un altro disco archivio.

Configurare un profilo collector

N.B.: per impostazione predefinita, le impostazioni di configurazione del software di valutazione sono impostate per non raccogliere nessun file. Specificare un sottoinsieme ristretto di tutti i file sul dispositivo di destinazione per ridurre il tempo di raccolta e non superare la capacità del collector.

La configurazione di un collector permette all'utente di determinare una serie di tipi di file o file specifici creati tra un set specifico di dati che il collector estrarrà dal dispositivo di storage sospetto per la valutazione. Quanto più si è in grado di restringere la raccolta di parametri, tanto più rapidamente i dati di destinazione possono essere acquisiti per la revisione.

Dell consiglia la creazione di un insieme di profili di configurazione standard che voi o la vostra agenzia riscontra ripetutamente. Esempi di tali profili di configurazione standard sono i seguenti:

- Foto e video verranno raccolti per tipi di file quali *.**jpg**, *.**png**, *.**swf**, *.**vob**, e *.**wmv**, associati a fotografie, video o altri tipi di supporti visivi
- I documenti verranno più specificatamente raccolti per tipi di file quali *.**pdf**, *.**doc**, *.**docx**, *.**txt**.
- Audio_Files verranno raccolti per *.**mp3**, *.**mp4**, *.**wav**, altri tipi di file.

Configurazione di un collector per l'acquisizione

N.B.: per una spiegazione sulle differenze tra acquisizione standard e Live, consultare "Acquisizione standard vs. Acquisizione Live" a pagina 20.

N.B.: quando un collector viene configurato per l'acquisizione standard o live, deve essere pulito prima di potere essere configurato per l'uso in un altro tipo di acquisizione.

1 Dal **Collector Menu**, sfiorare o fare clic su **Configure Collector**.

Figura 2-8. Menu collector

2 Se si è creato in precedenza un profilo di configurazione che si desidera utilizzare, selezionare il profilo e sfiorare o fare clic su **Configure using selected profile** per iniziare la configurazione del collector, altrimenti, sfiorare o fare clic su **New** per creare un nuovo profilo.

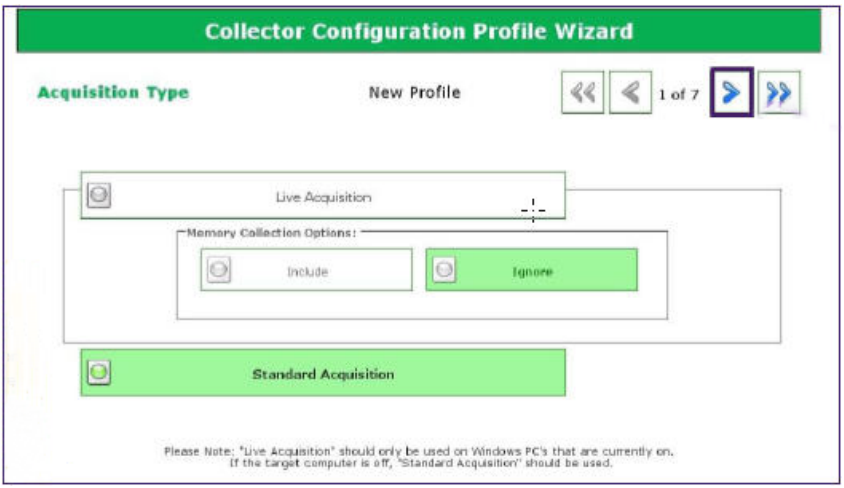
N.B.: Figura 2-9 mostra la schermata **Selected Profile** al primo utilizzo del software prima che qualsiasi profilo sia definito o salvato. Quando si è avviata la creazione dei profili, verranno visualizzati nella schermata per essere utilizzati.

N.B.: la navigazione da una schermata della Configurazione del collector alla successiva viene realizzata sfiorando i pulsanti freccia destra o sinistra in alto e al lato della schermata.

Figura 2-9. Seleziona profilo

3 Determinare il tipo di acquisizione che si desidera eseguire, Live o standard (consultare "Acquisizione standard vs. Acquisizione Live" a pagina 20 per ulteriori informazioni sulla differenze tra i tipi di acquisizione Live e standard), quindi sfiorare o fare clic su **Live Acquisition** o **Standard Acquisition**.

Figura 2-10. Passaggio 1 della configurazione del profilo: tipo di acquisizione


Collector Configuration Profile Wizard
Acquisition Type
New Profile
1 of 7
Live Acquisition
Memory Collection Options:
Include
Ignore
Standard Acquisition
Please Note: "Live Acquisition" should only be used on Windows PC's that are currently on.
If the target computer is off, "Standard Acquisition" should be used.

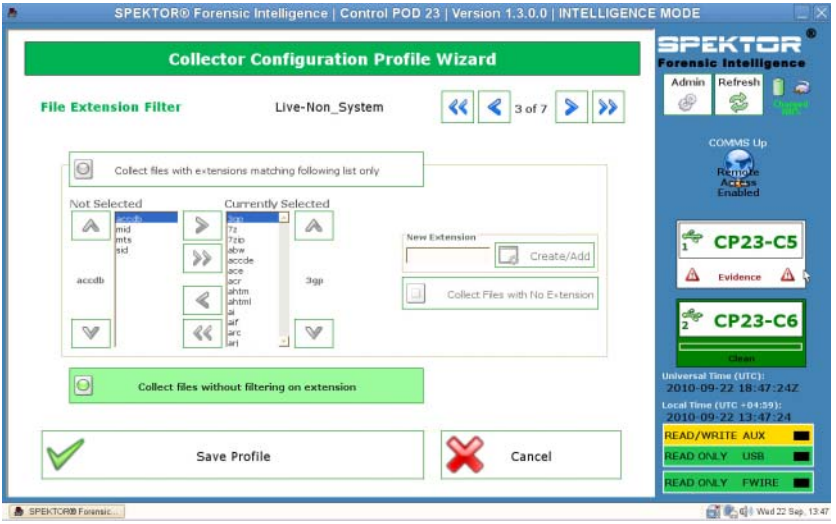
4 Determinare le impostazioni timestamp per il nuovo profilo. Quanto più specifici si è, tanto più breve sarà il tempo necessario per elaborare i file acquisiti.

Figura 2-11. Passaggio 2 della configurazione del profilo: impostazioni timestamp del file

5 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata.

6 Nella schermata **File Extension Filter**, selezionare i tipi di file che si desidera raccogliere. Utilizzare la freccia destra per spostare i tipi di file selezionati e le estensioni associate dalla casella **Not Selected** alla casella **Currently Selected**.

Figura 2-12. Passaggio 3 della configurazione del profilo: filtro estensione file



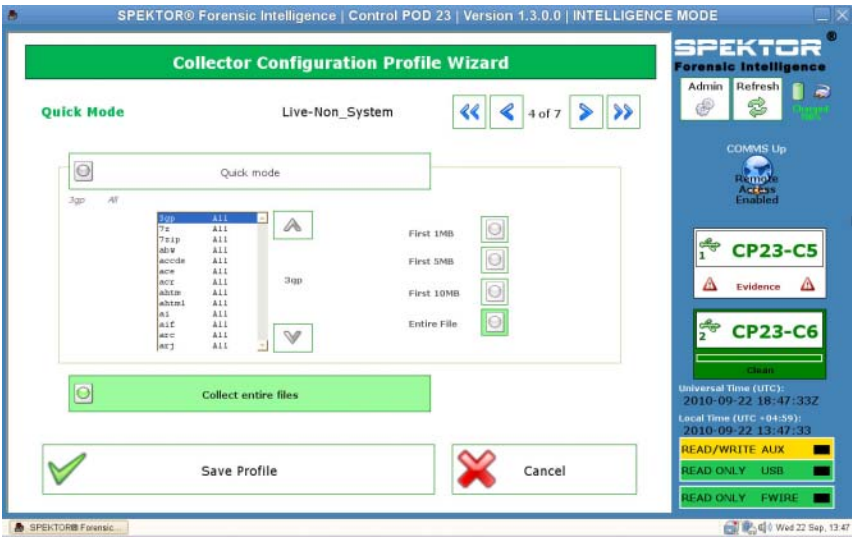
7 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata quando si è terminata la selezione dei tipi di file e delle estensioni.

N.B.: solo se specificatamente richiesto, si consiglia di lasciare la modalità rapida disattivata.

8 Nella schermata **Quick Mode**, selezionare il numero di megabyte (**1 MB**, **5 MB**, **10 MB**, o **Intero file**) della prima parte dei file che si desidera acquisire. Raccogliendo solo la prima parte di file molto grandi (tipicamente file multimediali), è possibile revisionare una porzione sufficiente dei file per determinare il contenuto riducendo così la quantità di tempo di elaborazione necessaria.

N.B.: se non si sono selezionate le estensioni dei file nel passaggio 6, nessun file verrà raccolto e nessun tipi di file verrà visualizzato per la selezione in questa schermata. Ritornare a punto 6 e selezionare i tipi di file richiesti per prepararsi per il passaggio 8.

Figura 2-13. Passaggio 4 della configurazione del profilo: modalità rapida



9 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata.

10 Sfiorare o fare clic sul pulsante appropriato per selezionare qualsiasi file del sistema che si desidera includere nella raccolta.

Figura 2-14. Passaggio 5 della configurazione del profilo: file di sistema

11 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata.

12 Nella schermata **Deleted File Filter**, determinare se si desidera includere o meno nella raccolta i file live ed eliminati, solo file live o solo file eliminati. Se non si seleziona nessuna di queste opzioni, non si raccoglierà alcun file.

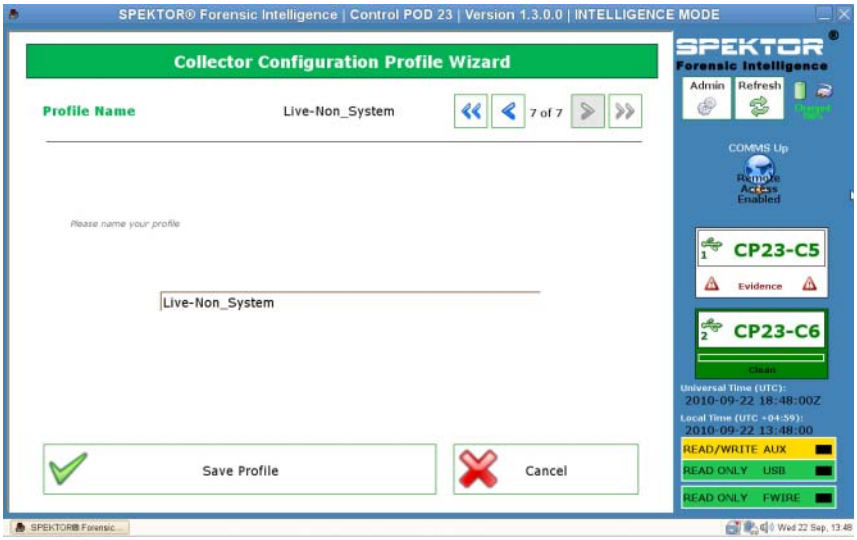
Figura 2-15. Passaggio 6 della configurazione del profilo: filtro estensione file

N.B.: solo i file eliminati che non sono stati sovrascritti già presenti sul dispositivo di destinazione possono essere raccolti con successo. I file eliminati e sovrascritti potranno essere corrotti o non ripristinabili.

13 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata.

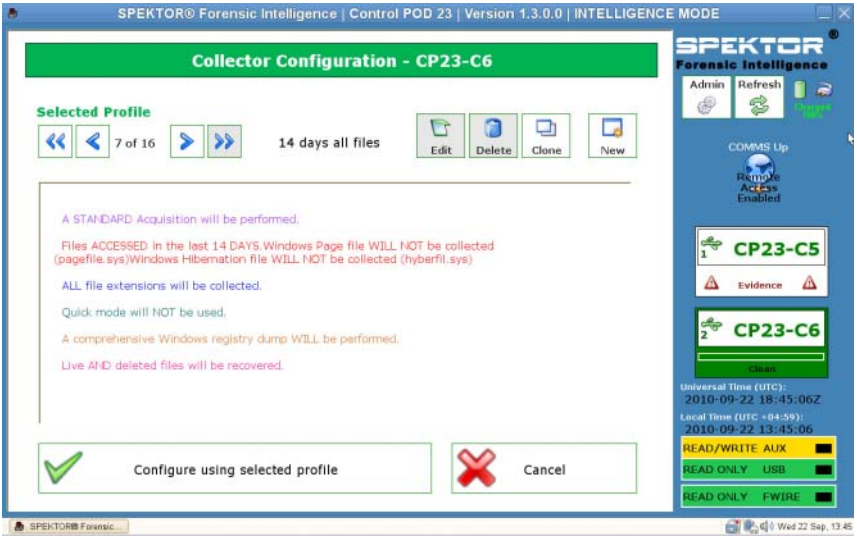
14 Nella schermata **Profile Name**, inserire il nome del nuovo profilo quindi sfiorare o fare clic su **Save Profile**.

Figura 2-16. Passaggio 7 della configurazione profilo: nome profilo



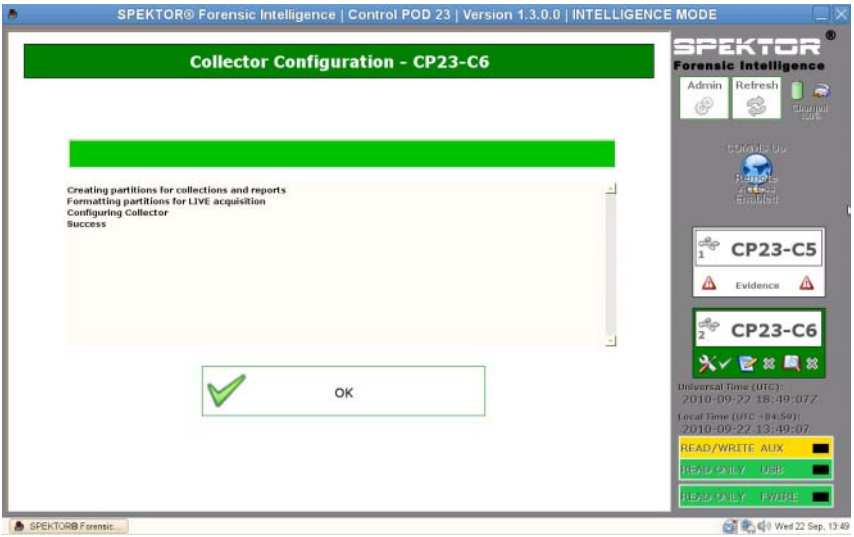
15 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata. Il nuovo profilo viene visualizzato nella schermata **Profilo selezionato**. La schermata **Collector Configuration** visualizzerà il titolo del profilo (in questo caso, **14 days all files**) ed elencherà i dettagli del profilo nella porzione principale della finestra.

Figura 2-17. Profilo selezionato dopo la creazione del profilo



16 Sfiorare o fare clic su **Configure using selected profile** per iniziare la configurazione del collector.

Figura 2-18. Profilo selezionato dopo la creazione del profilo



17 Sfiorare o fare clic su **OK** per iniziare la configurazione di collector. Questo processo durerà solo un minuto o due minuti.

Quando la configurazione del collector viene completata, il collector è pronto per essere utilizzato a confronto con il computer di destinazione o il dispositivo di storage di destinazione. (Consultare "Utilizzare strumenti di valutazione" a pagina 33).

18 Fare clic sulla freccia destra nell'angolo in alto a destra della schermata.

Utilizzare strumenti di valutazione

N.B.: per le differenze tra l'acquisizione Live e standard, consultare "Acquisizione standard vs. Acquisizione Live" a pagina 20.

N.B.: sebbene sia possibile utilizzare un collector per diversi casi, le best practice consigliano vivamente che ogni collector contenga solo i dati relativi ad un singolo caso, anche se i dati da dispositivi di storage da quel singolo caso possono essere memorizzati sul collector.

Utilizzare un collector per l'acquisizione standard a confronto con un computer di destinazione

AVVERTENZA: è necessario modificare l'ordine di avvio del sistema dall'interno del sistema BIOS del computer di destinazione prima di tentare un'acquisizione standard. Se il computer di destinazione è impostato per l'avvio dal disco rigido anziché dall'unità ottica con il disco di avvio SPEKTOR in posizione, i contenuti del disco del computer di destinazione verranno alterati. Assicurarsi di sapere come accedere al BIOS del sistema del computer di destinazione prima di accendere il computer di destinazione.

AVVERTENZA: prima di accendere il computer di destinazione, assicurarsi di aver inserito il disco di avvio SPEKTOR nell'unità ottica su cui è impostato il computer di destinazione per l'avvio. Il mancato avvio del computer di destinazione senza il disco di avvio comporterà l'alterazione dei contenuti del disco del computer di destinazione.

N.B.: occorre avere un disco di avvio di SPEKTOR per eseguire un'acquisizione standard a confronto di un computer di destinazione. Consultare "Masterizzare un CD di avvio per le procedure di acquisizione standard" a pagina 21 per ulteriori informazioni sulla creazione di un disco di avvio.

1. Sul portatile Dell rugged, sfiorare o fare clic su **Deploy Collector**.
2. Selezionare **Target Computer**.
3. Fare clic su **OK**, quindi scollegare il collector dal portatile Dell rugged.
4. Collegare il collector ad una porta USB disponibile sul computer di destinazione.

N.B.: Dell consiglia di utilizzare sempre l'unità ottica interna del computer di destinazione con il disco di avvio. Se ciò non è possibile, utilizzare un'unità ottica esterna con un connettore USB.

5. Posizionare il disco di avvio di SPEKTOR nell'unità ottica.
6. Accedere al programma del sistema BIOS del computer di destinazione e cambiare l'ordine di avvio in modo che il computer di destinazione sia avviato dall'unità ottica.

   Il disco di avvio di SPEKTOR si avvierà e verrà visualizzata l'interfaccia unità di avvio.
7. Inserire le informazioni richieste sulla schermata, premendo <Enter> o i tasti freccia per spostarsi tra i campi, quindi spostarsi nel campo **COLLECT** e premere <Enter> per iniziare la raccolta dei dati.

ATTENZIONE: non rimuovere il disco di avvio di SPEKTOR dall'unità ottica fino a che il computer di destinazione sia spento completamente.

8 Quando il processo di raccolta viene completato, premere <Enter> per spegnere il computer di destinazione.

9 Rimuovere il disco di avvio di SPEKTOR dall'unità ottica, scollegare il collector dalla porta USB dal computer di destinazione e collegarlo alla porta USB disponibile sul portatile Dell rugged.

Utilizzare un collector per l'acquisizione standard in confronto con un dispositivo di storage di destinazione

1 Collegare il dispositivo di storage di destinazione ad una porta USB di sola lettura o alla porta firewire del portatile Dell rugged.

2 Sfiorare o fare clic su **Deploy Collector**.

3 Sfiorare o fare clic su **Target Storage Device**, inserire le informazioni richieste, quindi sfiorare o fare clic su **Collect from Device**.

4 Quando la raccolta è completata, scollegare il dispositivo di storage di destinazione dalla porta USB e sfiorare o fare clic su **OK**.

Utilizzare un collector per un'acquisizione Live

N.B.: assicurarsi di prendere note precise e dettagliate durante questa procedura, come parte delle best practice per la catena di custodia.

N.B.: non serve che il disco di avvio di SPEKTOR termini l'utilizzo di un'acquisizione Live.

1 Fare clic su **Deploy Collector→ Target Computer**.

2 Sul dispositivo di destinazione, navigate fino a **My Computer** (o **Computer** sui computer con sistema operativo Windows Vista o Windows 7).

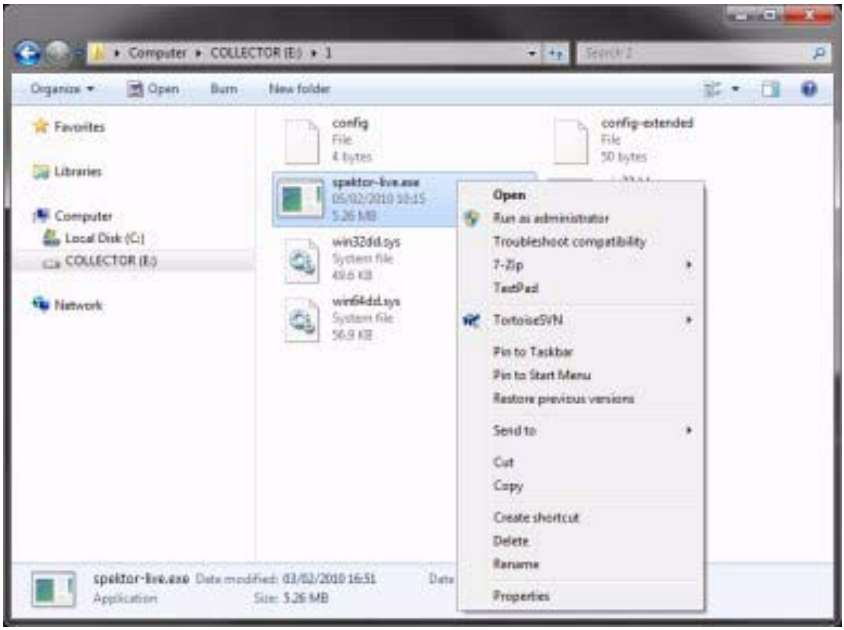
3 Fare doppio clic sull'icona **Collector** che viene visualizzata per visualizzare i contenuti del collector.

Figura 2-19. Icona Collector

4 Fare clic sulla cartella nominata con il numero più elevato. Verrà visualizzata solo una cartella se questo è il primo utilizzo dalla pulizia di questo collector.

5 Fare clic con il tasto destro del mouse su **spektor-live.exe**, quindi selezionare **Run as administrator** nella casella a discesa. Se si visualizza un messaggio che richiede di riconoscere le autorizzazioni per eseguire l'applicazione come amministratore, fare clic su **Continue**.

Figura 2-20. Eseguire come amministratore.



6 Inserire le informazioni richieste nella schermata **SPEKTOR Live Collection**, quindi fare clic su **Run**.

7 Quando richiesto, fare clic su **Chiudi**.

8 Scollegare il collector dal dispositivo di destinazione e archiviarlo in modo sicuro per la successiva ingestione nel datacenter.

Revisione dei file raccolti dopo la valutazione

1 Dal **Collector Menu**, fare clic su **Reporting**. Questa opzione indicizza i dati raccolti e crea un set di report automaticamente.

2 Dalla schermata **Collector Collections**, selezionare **Main Report**, quindi fare clic su **Generate Selected Reports**.

Figura 2-21. Generare report

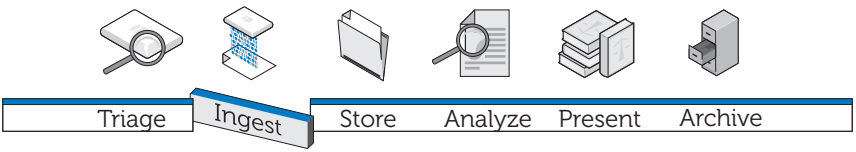
3 Fare clic su **OK** quando il processo di generazione di report è completo per ritornare al menu **Reporting**.

N.B.: fare riferimento al *Manuale dell'utente* di SPEKTOR per maggiori informazioni sulla creazione e l'esportazione di report utilizzando criteri specifici. Consultare "Documentazione e risorse correlate" a pagina 16.

4 Fare clic su **View Collection Report** per rivedere i report, quindi fare clic su una delle cinque categorie di report, **Images**, **Documents**, **Multimedia**, **Other** o **System**, per visualizzare gli specifici report.

3

Ingerisci



La fase Ingerisci della soluzione Dell Digital Forensics consiste nel creare un'immagine del dispositivo di archiviazione di destinazione (se non è già stato fatto durante la fase di Valutazione), e quindi nel successivo trasferimento di quell'immagine in una posizione centrale da cui si può accedere per l'analisi. Per spostare le applicazioni Forensics nel datacenter e conservare ancora l'esperienza utente standard, Dell, in collaborazione con Citrix, ha creato diversi pacchetti software distinti per le applicazioni Forensics mainline per spostarle senza interruzione delle attività nel datacenter, creando un'esperienza utente più disponibile, più veloce e più capace.

Come parte della soluzione Digital Forensics, Dell ha attualmente certificato le seguenti applicazioni Forensics:

- SPEKTOR
- EnCase 6
- FTK 1.8
- FTK 3 versione standalone
- FTK 3 Lab Edition

Nessuna di queste applicazioni Forensics può essere utilizzata in combinazione per un accesso simultaneo ad un singolo dispositivo utente.

EnCase 6 abilitato per datacenter

Nell'esempio seguente soluzione, l'applicazione EnCase 6 è ospitata su dispositivi server Dell nel datacenter e garantisce sessioni EnCase 6 multiutente.

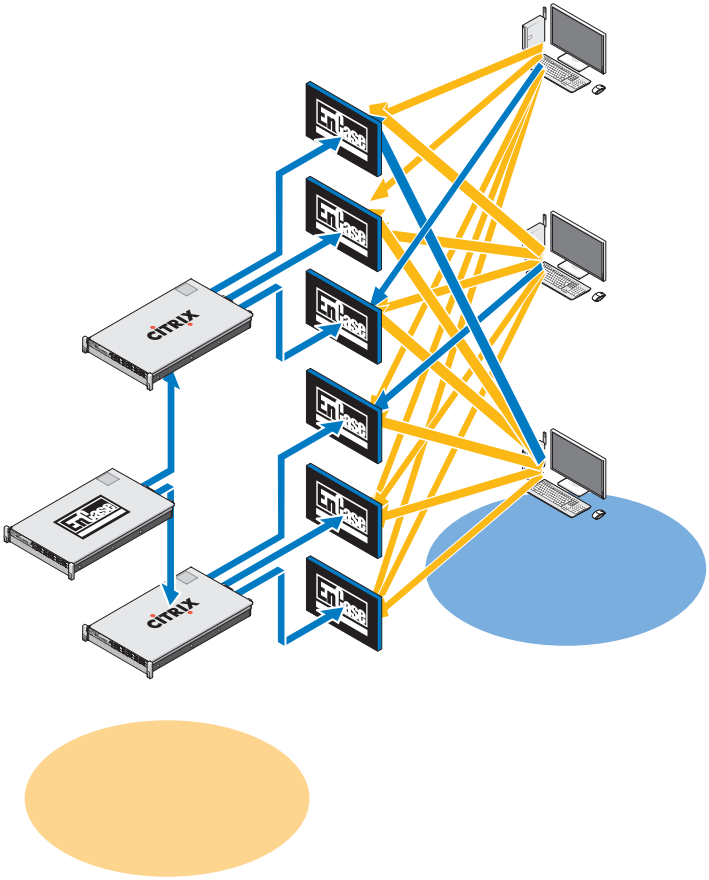
Soluzione singolo server

Nella soluzione singolo server EnCase 6, più client possono connettersi ad un unico server. Tutti i client sono puntati su questo server e non possono connettersi a nessun altro server EnCase 6. In caso di guasto del server, tutte le connessioni client andranno perse.

Soluzione multi-server (High Availability)

Nella soluzione multiserver, un utente si connetterà all'applicazione EnCase 6 sul farm Citrix e verrà indirizzato senza interruzione delle attività al server EnCase 6 attualmente al lavoro con il carico più leggero. Nel caso in cui l'utente esegue più istanze del software EnCase 6, ogni istanza può essere creata da un altro server. L'esperienza dell'utente risulta preservata, perché l'utente è totalmente ignaro del modo in cui vengono create più istanze, e tutte le sessioni sembrano essere in esecuzione sullo stesso server con lo stesso look and feel.

Figura 3-1. Schematica server/client EnCase 6 abilitato per datacenter



In caso di guasto del server, l'utente deve fare clic sull'icona EnCase sul desktop, e il sistema reindirizza la connessione utente al successivo server disponibile che fa da host a EnCase 6. Ogni server EnCase può supportare *x* sessioni utente, in cui *x* = *(numero di core x 2)*. Ogni sessione utente richiede 3 GB di RAM del server.

FTK 1.8 abilitato per datacenter

Nella soluzione FTK 1.8 abilitato per datacenter, i dispositivi server Dell fanno da host all'applicazione nel datacenter, garantendo sessioni FTK 1.8 multiutente (un'unica sessione utente per server).

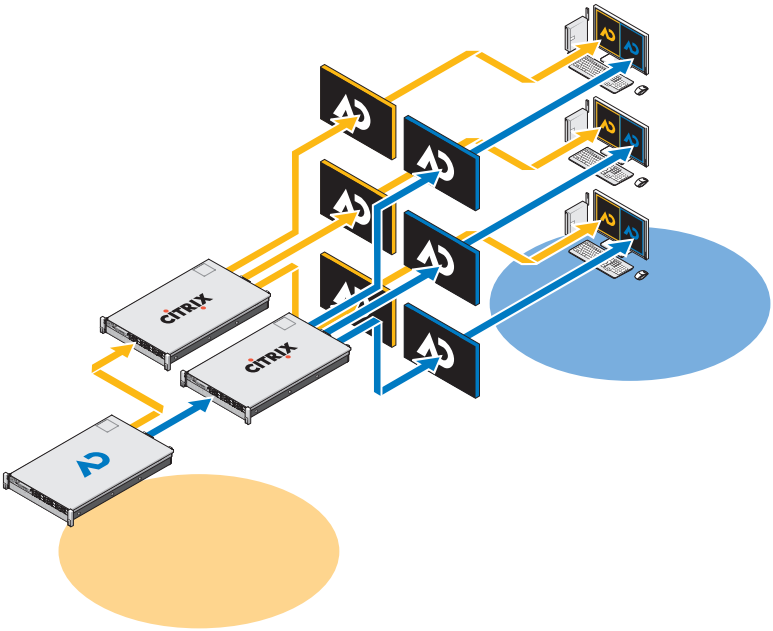
Sessione FTK 1.8 singola per desktop

Nella soluzione di singolo server FTK 1.8, client multipli possono connettersi ad un singolo server. Tutti i client sono puntati su questo server e non possono connettersi a nessun altro server FTK 1.8. In caso di guasto del server, tutte le connessioni client andranno perse. L'utente può eseguire solo una sessione di FTK 1.8 per ogni account utente di Windows.

Sessioni FTK 1.8 multiple per desktop

Nella soluzione multiserver FTK 1.8, un utente si connetterà al server FTK 1.8 utilizzando multiple icone del desktop FTK Server1, Server2 FTK, ecc. Ogni link è associato ad un server specifico. Per scopi illustrativi Figura 3-2 mostra il bordo della sessione del server FTK 1.8 in esecuzione con barre di colori al server che esegue la sessione di FTK 1.8 (server1= blu, server2 = rosso). Non è possibile eseguire due sessioni dell'applicazione FTK 1.8 dallo stesso server utilizzando lo stesso account utente. L'esperienza dell'utente dell'applicazione basata sul server FTK 1.8 è la stessa tra i client.

Figura 3-2. Schematica server e client FTK 1.8 multipli



In caso di guasto del server, l'utente perde l'accesso alla sessione server FTK 1.8 corrispondente. In questo caso, l'utente dovrebbe continuare a lavorare utilizzando gli altri server FTK. Tutte le informazioni e le prove caso (supponendo che l'utente abbia i privilegi di accesso NAS) sono disponibili presso tutte le sessioni del server FTK 1.8 attraverso NAS/SAN condivisa.

Ogni server FTK 1.8 può supportare *x* sessioni utente, in cui *x* = *(numero di core x 2)*. Ogni sessione utente richiede 3 GB di RAM del server e prestazioni del disco del datacenter pari a 1000 I/O per secondo.

FTK 3 abilitato per datacenter

Nella soluzione FTK 3 abilitato per datacenter, i dispositivi server Dell fanno da host all'applicazione nel datacenter, garantendo una singola sessione per server FTK 3.

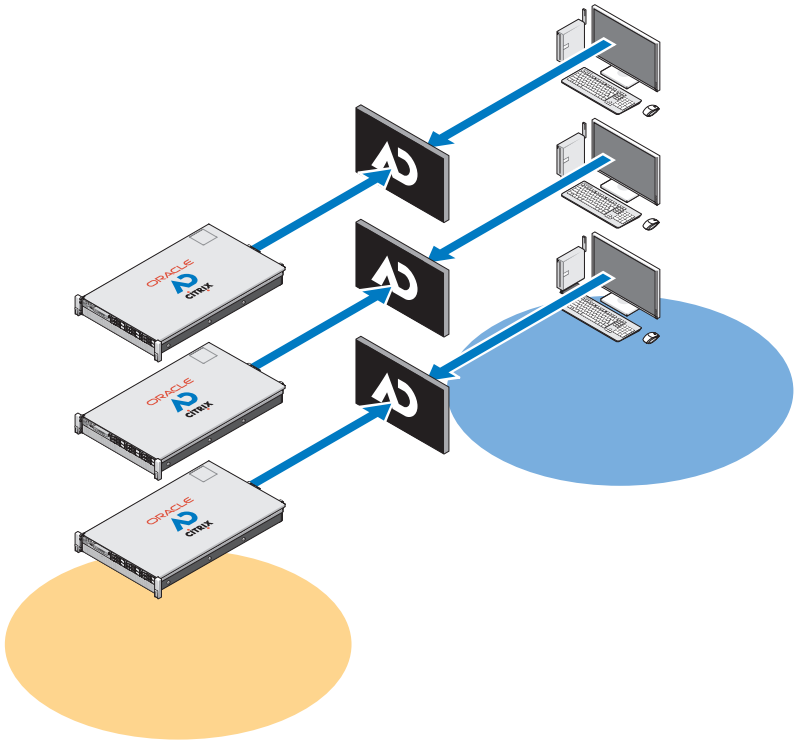
Soluzione server FTK 3 singola

Nella soluzione server FTK 3 singolo, un singolo client FTK 3 non può connettersi ad un server singolo. Tutti i client sono puntati su questo server e non possono connettersi a nessun altro server FTK 3. In caso di guasto del server, tutte le connessioni client andranno perse. Il server FTK 3, inoltre, eseguirà il database locale integrato FTK Oracle perché questa versione del database non supporta la collaborazione tra gli altri FTK database Oracle o di altri utenti FTK.

Soluzione multiserver (no High Availability)

Nella soluzione multiserver, ogni client si connetterà al proprio server FTK 3 home e non può connettersi a nessun altro server FTK 3. Quando un server dispone di una sessione di FTK 3 in esecuzione, non è più disponibile ad accettare nessuna nuova sessione del client FTK 3: l'installazione del software nella struttura Dell Forensics rende impossibile per un server eseguire più di una sessione di applicazione FTK 3 contemporaneamente. Consentendo solo una sessione in esecuzione per server, l'applicazione multithread FTK 3 è in grado di dedicare tutte le risorse del server disponibili per l'elaborazione di un caso, migliorando così le prestazioni.

Figura 3-3. Schematica server/client FTK 3 abilitato per datacenter



Con il software FTK Standard edition, ogni server deve eseguire una versione locale del database Oracle incluso in FTK (una versione del database Oracle per utente simultaneo). Questa versione dell'applicazione FTK e del database Oracle non supporta la collaborazione tra gli utenti FTK o altri database Oracle FTK.

Ogni database Oracle ha un agent di backup Oracle sul server e viene eseguito il backup del database come parte del normale regime di backup (consultare "Archivia" a pagina 83 per ulteriori informazioni)

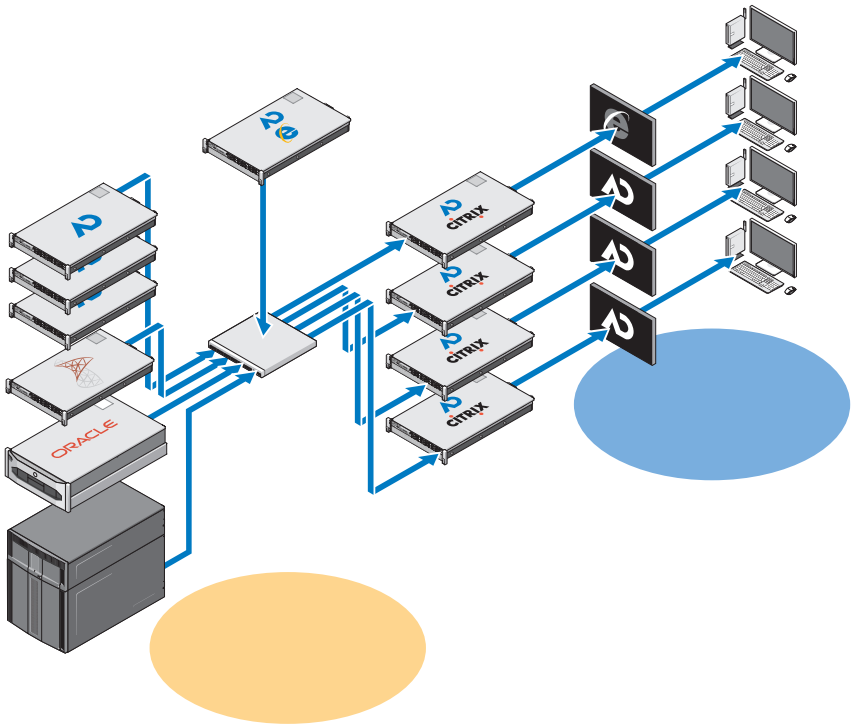
In caso di guasto del server, l'utente deve connettersi manualmente ad un altro server FTK 3 disponibile (se i server n +1 FTK 3 sono disponibili). Tuttavia, nel caso in cui anche il database Oracle abbia mostrato un errore, non sarà possibile l'accesso ai casi già elaborati, preesistenti casi poiché questi saranno collegati specificamente al database Oracle originale locale FTK 3 per quell'utente.

Ogni server FTK 3 può supportare una sessione utenti simultanei. Ogni sessione utente richiede 64 GB di memoria RAM del server (48 GB per Oracle e 16 GB per FTK) e 1000 + I/O al secondo per l'archivio di file più 600 + I/O al secondo per il database (configurazione minima).

FTK 3, Lab Edition

Nella configurazione FTK 3 Lab Edition, l'utente si connette ad un server che fa da host ad AccessData Lab e al database dei casi centralizzato. Più utenti possono accedere allo stesso caso contemporaneamente ed anche eseguire analisi diverse nello stesso momento. L'elaborazione viene gestita utilizzando un modello di elaborazione distribuita.

Figura 3-4. Schematica client e server FTK 3 Lab Edition



Lo storage del caso è ottimizzato utilizzando un mix di hardware SAS e SATA, e l'intero datacenter Forensics possono essere gestiti centralmente da un responsabile amministrativo.

Molteplici applicazioni Forensics fornite in un desktop

Nella soluzione multivendor e multiapplicazione, tutte le soluzioni applicative individuali descritte in precedenza sono combinate per fornire all'analista della scientifica l'accesso a tutte le applicazioni Forensics (EnCase 6, FTK 1.8 FTK e 3, o FTK 3 Lab Edition) da un singolo desktop o anche un singolo riquadro. Tutte le applicazioni possono essere fornite in modalità high availaibility in modo che in caso di guasto, l'utente abbia comunque accesso a quella specifica applicazione, e, nel caso di FTK 1.8, l'utente abbia comunque accesso utilizzando uno delle altre icone FTK 1.8 sul desktop.

Consigli sulla configurazione di rete

Tabella 3-1. Struttura indirizzo IP consigliata

Indirizzo IP	Funzione server	Nome server
192.168.1.1	Controller di dominio 1	DF-DC1
192.168.1.2	Controller di dominio 2	DF-DC2
192.168.1.3	Server prove	prove DF
192.168.1.4	Server dello spazio di lavoro	Spazio di lavoro DF
192.168.1.5	Server Oracle FTK	DF-FTK
10.1.0.0/24	Range indirizzo IP statico 1 GB	
10.1.1.0.0/24	Range indirizzo IP statico 10 GB	
10.1.2.0/24	Range DHCP di 1 GB DHCP, client	
10.1.0.250-254	Switch da 1 GB	
10.1.1.250-254	Switch da 10 GB	
10.1.0.200	Server DNS	

Tabella 3-2. Convenzioni per la nominazione consigliate per i server della soluzione

Nome	Abbreviazione
Nome dominio	DF (Digital Forensics)
Controller di dominio 1	DF-DC1
Controller di dominio 2	DF-DC2
Storage prove	Prove DF
Spazio di lavoro	Spazio di lavoro DF
Oracle	DF-Oracle
SQL	DF-SQL
FTK-Lab	FTK-Lab
FTK-Standalone	FTK
Gestori di elaborazione continua	DF-DPM, DF-DPM1, DF-DPM2
Motore di elaborazione distribuita	DF-DPE, DF-DPE1, DF-DPE2

Tabella 3-3. Convenzioni di nominazione consigliate per NIC Teaming

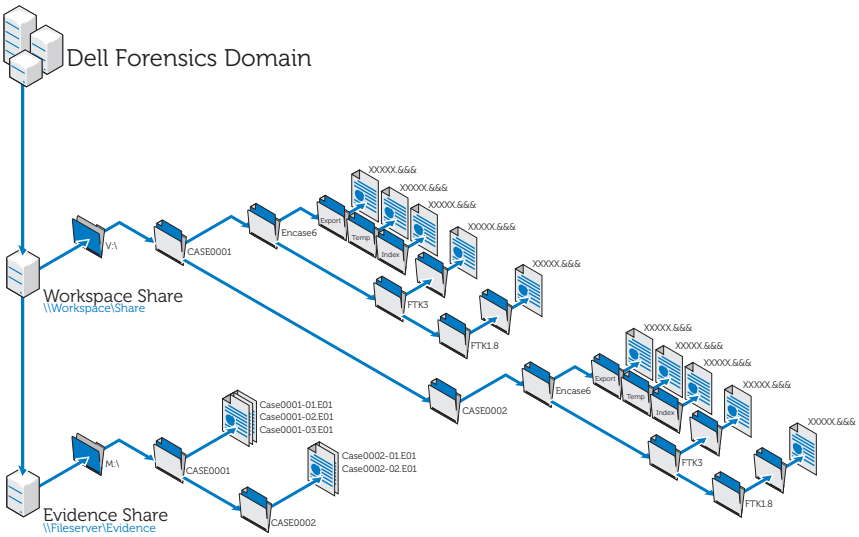
NIC Team 1	Rete pubblica	Per server connessi uno all'altro
NIC Team 2	iSCSI	Per server connessi ai dispositivi di storage EqualLogic

Tabella 3-4. Struttura di mapping della lettera dell'unità consigliata

Nome chiamata	Unità	Locale o SAN	RAID	Note
Unità locale	C	Locale	RAID1 (dischi 2xSAS da 15 K)	
	D:	Locale		
CD-ROM	E:			
	F:			
	G:			
SQL	H:	SAN	RAID0+1	Non su dischi SATA
Oracle	I:	SAN	RAID0+1	Non su dischi SATA
Unità EV Vault	J:	SAN	RAID50	
Backup su disco	K:	SAN	RAID50	
Riserva	L:	SAN	RAID50	
Prova 1	M:	SAN	RAID50	
Prova 2	N:	SAN	RAID50	
Prova 3	O:	SAN	RAID50	
Prova 4	P:	SAN	RAID50	
Prova 5	Q:	SAN	RAID50	
Prova 6	R:	SAN	RAID50	
Prova 7	S:	SAN	RAID50	

Nome chiamata	Unità	Locale o SAN	RAID	Note
Prova 8	T:	SAN	RAID50	
Prova 9	U:	SAN	RAID50	
Spazio di lavoro 1	V:	SAN	RAID50	
Spazio di lavoro 2	W:	SAN	RAID50	
Spazio di lavoro 3	X:	SAN	RAID50	
Spazio di lavoro 4	Y:	SAN	RAID50	
Spazio di lavoro 5	Z:	SAN	RAID50	

Figura 3-5. Struttura file consigliata da Dell



Come eseguire l'ingestione con la soluzione Dell Digital Forensics

Ingerisci con SPEKTOR

Registrare e pulire un dispositivo esterno come disco archivio

1. Collegare il dispositivo USB esterno non registrato ad una porta per collector sul portatile rugged.
2. Sfiorare o fare clic sull'icona del dispositivo quando viene visualizzato; quindi sfiorare o fare clic su **Register the Device as a Store Disk→ Yes**. Inserire le informazioni richieste.
3. Dal menu a destra, selezionare il dispositivo registrato quindi sfiorare o fare clic su **Clean/Reformat→ Clean**.
4. Fare clic su **OK** quando il processo viene completato.

Utilizzare il disco archivio

1. Collegare il disco archivio al portatile rugged quindi sfiorare o fare clic sul dispositivo disco archivio per visualizzare il **Store Disk Menu**.
2. Nel **Store Disk Menu**, sfiorare o fare clic su **Deploy**.

   Se si sta utilizzando a confronto con un computer di destinazione:

   a. Sfiorare o fare clic su **Target Computer**.

   b. Rimuovere il disco archivio dal computer portatile rugged e inserirlo in una porta USB sul computer di destinazione.

   c. Seguire le istruzioni di utilizzo come per catturare un'immagine in "Utilizzare strumenti di valutazione" a pagina 33.

   d. Quando il CD di avvio viene caricato, **SPEKTOR Imaging Wizard** guiderà l'utente lungo il resto del processo di creazione dell'immagine. Istruzioni passo dopo passo possono essere ritrovate nel *Manuale dell'utente SPEKTOR*. Per ulteriori informazioni, consultare "Documentazione e risorse correlate" a pagina 16.

   e. Spegnere il computer di destinazione, scollegare il disco archivio, e quindi riportare il disco archivio nel datacenter per lo storage.

Se si utilizza a confronto con un dispositivo di storage di destinazione a livello locale:

a Sfiorare o fare clic su **Target Storage Device**.

b Collegare il dispositivo di storage di destinazione ad una porta USB di sola lettura o alla porta sulla destra del portatile rugged.

c Selezionare le partizioni o l'unità per cui si desidera creare l'immagine e quindi fare clic sulla freccia destra nell'angolo in alto a destra della schermata.

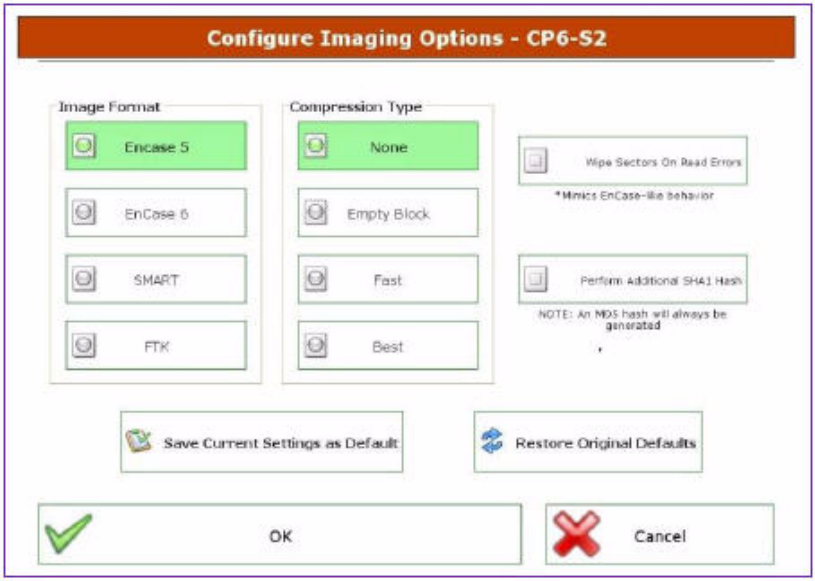
d Inserire le informazioni del caso richieste e quindi sfiorare o fare clic su **Image Now**.

e Se necessario, sfiorare o fare clic su **Configure Imaging Options** per cambiare il **Image Format** o il **Compression Type**, o per **Wipe Sectors on Read Errors** o **Perform Additional SHA1 Hash**.

N.B.: un hash MDS verrà sempre generato durante il processo di imaging.

N.B.: consultare il *Manuale dell'utente di SPEKTOR* per maggiori informazioni su ognuna di queste opzioni di imaging. Consultare "Documentazione e risorse correlate" a pagina 16.

Figura 3-6. Configurare le opzioni di imaging



f Sfiorare o fare clic su **Image Now→ Yes** per avviare il processo di imaging.

g Quando il processo di imaging viene completato, sfiorare o fare clic su **OK**.

h Scollegare il dispositivo di storage di destinazione e il disco archivio dal portatile rugged; quindi riportare il disco archivio nel datacenter per lo storage e l'analisi.

N.B.: il trasferimento di un'immagine può richiedere molto tempo, sei ore per un tipico trasferimento 60 GB di disco rigido non è un valore insolito.

Ingerisci con EnCase

Nella soluzione Dell Digital Forensics, la licenza per EnCase è realizzata utilizzando un sistema di licenze di rete. Tipicamente, un'istanza di EnCase SAFE viene installata su uno dei server del datacenter e un dongle contenente licenze multiple viene connesso al server. I client EnCase sono configurati per guardare a quel server per le licenze, e non sono necessari dongle locali. Consultare la *Guida alla configurazione e all'installazione di Dell Digital* per maggiori informazioni. Consultare "Documentazione e risorse correlate" a pagina 16. Inoltre, consultare l'amministratore dei sistemi di rete per informazioni specifiche sull'installazione della soluzione proprie dell'agenzia per cui si lavora.

1 Collegare il dispositivo di storage di destinazione alla workstation nel datacenter appropriata per l'ingestione.

a Se si sta creando un'immagine di un'unità SATA, consultare "Connessione del Tableau Write-Blocker al disco rigido SATA" a pagina 55 per maggiori informazioni.

b Se si sta creando un'immagine di un'unità IDE, consultare "Connessione del Tableau Write-Blocker al disco rigido IDE" a pagina 55 per maggiori informazioni.

2 Creare un nuovo caso.

N.B.: le istruzioni che seguono si riferiscono alla struttura della rete e delle cartelle delineata come best practice suggerite da Dell per la soluzione Digital Forensics; consultare Figura 3-5 per maggiori informazioni.

a Fare clic su **New**, quindi inserire le informazioni richieste.

b Nell'unità **W:\ drive** (area di lavoro), creare le cartelle utilizzando la seguente struttura:

- `W:\[CaseName]\EnCase6\Export`
- `W:\[CaseName]\EnCase6\Temp`
- `W:\[CaseName]\EnCase6\Index`

c Fare clic su **Finish**.

d Fare clic su **Sì** per ogni richiesta per creare la cartella.

e Nella schermata **EnCase Acquisition**, fare clic sull'opzione di menu **Add Device**.

f Assicurarsi che la casella **Sessions** sia selezionata.

g Nel riquadro a destra, selezionare il proprio caso.

h Fare clic su **Add Evidence Files**, quindi navigare fino al repository E01 (utilizzando la configurazione con le best practice indicate in Figura 3-5, questo repository deve essere memorizzato sull'unità **X:**\).

i Fare clic su **Next**→ **Next**→ **Finish**. Un'icona del cronometro appare nella parte inferiore destra della schermata **Acquisition** EnCase, e EnCase verificherà il file E01. A seconda delle dimensioni del file, la verifica può richiedere del tempo.

3 All'interno del software EnCase, aggiungere il dispositivo di storage di destinazione utilizzando la procedura guidata **Aggiungi dispositivo**.

4 Acquisire il contenuto del dispositivo.

a Dal software EnCase, fare clic su **Cases**→ **Entries**→ **Home**; quindi fare clic con il tasto destro del mouse sul dispositivo che si desidera acquisire.

b Selezionare **Acquire** dal menu a discesa.

c Nella casella **After Acquisition**, selezionare il tipo di file **New Image File**:

- **Non aggiungere** le opzioni che escludono l'immagine acquisita di recente dal caso al momento aperto.
- **Add to Case** aggiunge immagine di recente acquisizione al file del caso associato al dispositivo su cui è stata catturata l'immagine.
- **Replace a source device** aggiunge l'immagine di recente acquisizione al caso e rimuove il dispositivo precedentemente visualizzato su cui è stata effettuata l'acquisizione.

d Fare clic su **Finish**. Quando il processo di creazione immagine è completato, viene visualizzata la casella **Acquisition Results**.

Lavorare con Tableau Write-Blockers

ATTENZIONE: non rimuovere un disco rigido da un ponte Forensics quando è presente l'alimentazione.

ATTENZIONE: non utilizzare estensioni dei cavi USB con alcun ponte Forensics.

Connessione del Tableau Write-Blocker al disco rigido SATA

1. Assicurarsi che **DC IN B** del ponte SATA/IDEe T35es Forensic sia in posizione **B On**.
2. Collegare la fonte di alimentazione TP2 o TP3 sul lato sinistro del ponte SATA T35es utilizzando il connettore mini-DIN da 5 piedini.
3. Collegare il cavo di alimentazione alla presa di corrente TP2 e anche ad una presa elettrica.
4. Accendere per verificare che il LED blocco di scrittura sia acceso, poi spegnere il ponte prima del collegamento al dispositivo di storage di destinazione.
5. Collegare il connettore Molex femmina del cavo di alimentazione SATA TC5 8 Style alla posizione **DC OUT** sul lato destro del ponte SATA/IDE T35es.
6. Collegare il connettore di alimentazione SATA del cavo di alimentazione SATA TC5 8 Style al connettore di alimentazione SATA del disco rigido di destinazione.

ATTENZIONE: utilizzando le connessioni Molex e SATA durante la connessione ad un dispositivo di storage di destinazione verrà sovraccaricato il dispositivo di destinazione.

7. Collegare il cavo di segnale SATA TC3 8 al ponte SATA/IDE T35es.
8. Collegare l'altra estremità del cavo di segnale SATA TC3-8 al dispositivo di storage di destinazione.
9. Collegare un'estremità del cavo dati (USB 2.0, due connessioni FireWire 800, connessione Orion FireWire 400 a 4 piedini) ad una delle porte sul lato sinistro del ponte SATA/IDE T35es.
10. Inserire l'altra estremità del cavo dati ad una porta sul computer portatile rugged Dell o sulla workstation Dell OptiPlex.
11. Spostare l'interruttore sulla parte superiore del ponte SATA/IDE T35es in posizione **A ON**. Il portatile Dell rugged o la workstation Dell OptiPlex dovrebbero registrare la presenza del dispositivo di storage di destinazione.

Connessione del Tableau Write-Blocker al disco rigido IDE

1. Assicurarsi che **DC IN B** del ponte SATA/IDEe T35es Forensic sia in posizione **B On**.
2. Collegare la fonte di alimentazione TP2 o TP3 al lato sinistro del ponte SATA/IDE T35es utilizzando il connettore mini-DIN da 5 piedini.

N.B.: il DIN a 7 piedini collegato all'alimentazione TP3 non funziona con i ponti Tableau. È necessario utilizzare il cavo adattatore da DIN a 7 piedini a DIN a 5 piedini TCA-P7-P5 per collegare l'alimentazione TP3 ai ponti Tableau.

3. Collegare il cavo di alimentazione alla presa di corrente TP2 e anche ad una presa elettrica.
4. Accendere l'alimentazione per verificare che il LED **blocco di scrittura** sia **ACCESO**; quindi **SPEGNERE** l'alimentazione del ponte prima del collegamento al disco rigido di destinazione.
5. Collegare un connettore Molex femmina del cavo di alimentazione Molex TC2-8 Style alla DC OUT situata sul lato destro del ponte SATA/IDE T35es.
6. Collegare l'altro connettore Molex femmina del cavo di alimentazione TC2-8 Molex Style al connettore Molex del disco rigido sospetto.
7. Collegare l'estremità blu del cavo di segnale TC6-8 IDE (in modo da allineare il piedino 1) al ponte SATA/IDE T35es.
8. Collegare l'estremità nera del cavo di segnale TC6-8 IDE al dispositivo di archiviazione di destinazione.
9. Collegare un'estremità del cavo dati (USB 2.0, due connessioni FireWire 800, connessione Orion FireWire 400 a 4 piedini) ad una delle porte sul lato sinistro del ponte SATA T35es.
10. Inserire l'altra estremità del cavo dati in una porta sul computer portatile Dell rugged o sulla workstation Dell OptiPlex.
11. Spostare l'interruttore sulla parte superiore del ponte SATA/IDE T35es in posizione **A On**. Il portatile Dell rugged o la workstation Dell OptiPlex dovrebbe riconoscere la presenza del dispositivo di storage di destinazione.

Ingerisci con FTK 1.8 e 3.0 abilitato per datacenter

Nella soluzione Dell Digital Forensics, la licenza per FTK è realizzata utilizzando un sistema di licenze di rete. Solitamente, il server di licenza di rete FTK è installato su uno dei server del datacenter, e un dongle FTK contenente licenze multiple è collegato a quel server. I client FTK sono configurati per guardare a quel server per le licenze, e non sono necessari dongle locali. Consultare la *Guida alla configurazione e all'installazione di Dell Digital Forensics* per maggiori informazioni. Consultare "Documentazione e risorse correlate" a pagina 16. Inoltre, consultare l'amministratore dei sistemi di rete per informazioni specifiche sull'installazione della soluzione proprie dell'agenzia per cui si lavora.

Creare un'immagine del dispositivo di storage di destinazione

1. All'interno dell'applicazione AccessData FTK Imager fare clic su **File**→ **Create Disk Image . . .**
2. Nel messaggio pop-up **Select Source**, selezionare il tipo di prove per cui si desidera creare un'immagine: Unità fisica, Unità logica, File immagine, Contenuti cartella o Dispositivo Fernico e quindi fare clic su **Next**.

N.B.: quanto segue utilizza l'opzione di **Imaging a Physical Drive** per dimostrare il processo di creazione dell'immagine. Le altre opzioni file sono descritte nella *Guida dell'uten***te** *FTK*. Consultare "Documentazione e risorse correlate" a pagina 16.

3. Utilizzando la casella a discesa selezionare l'unità fisica di cui si desidera creare un'immagine dalle unità disponibili, quindi fare clic su **Finish**.
4. Nel messaggio pop-up **Create Image**, fare clic su **Add . . .** e selezionare un tipo di immagine che si desidera creare (Raw, SMART, E01 o AFF). Fare quindi clic su **Next**.
5. Inserire le informazioni richieste nella finestra **Evidence Item Information** (Numero caso, Numero prova, Descrizione univoca, Esaminatore e Appunti). Fare quindi clic su **Next**.
6. Nella finestra **Select Image Destination**, sfogliare fino all'area di storage allocata per le immagini delle prove (consultare Figura 3-5 per la nomenclatura del server e dei file consigliata da Dell), inserire il nome del file di un'immagine,quindi fare clic su→
7. Fare clic su **Start**. Viene visualizzato il messaggio **Creating Image . . .** e propone la barra del progresso dell'operazione.

N.B.: la creazione del processo dell'immagine potrebbero richiedere delle ore in base al volume dei dati che si vanno ad aggiungere.

8. Se si è optato in precedenza per la visualizzazione di un riepilogo dei risultati dell'immagine, verrà visualizzata la finestra **Drive/Image Verify Results** al termine del processo di creazione dell'immagine. Rivedere i risultati e quindi fare clic su **Close**.
9. Fare clic di nuovo su **Close** per chiudere la finestra **Creating Image . . .**

Creare un caso

1. Fare clic su **File**→ **New Case**. Inserire quanto segue: **Nome investigatore**, **Numero caso**, **Nome caso**, **Percorso caso**, e **Cartella caso**.

2 Nella finestra **Forensic Examiner Information**, inserire quanto segue: **Agenzia/Azienda**, **Nome esaminatore**, **Indirizzo**, **Telefono**, **Fax**, **E-mail**, e **Commenti**. Fare quindi clic su **Next**.

3 Nella finestra **Case Log Options**, selezionare il set di opzioni che si desidera modificare:

- Eventi del caso e delle prove
- Messaggi di errore
- Creazione segnalibri per eventi
- Ricerca eventi
- Data carving/Ricerche Internet
- Altri eventi

4 Nella finestra **Processes to Perform**, selezionare i processi che si desidera eseguire. Selezionare i **Processes** dalle seguenti opzioni:

- Hash MD5
- Hash SHA1
- Ricerca KFF
- Test entropia
- Indice testo completo
- Archivia miniature
- Decifra fil EFS
- Database elenco file
- Elenco file HTML
- Data Carve
- Report di registro

5 Fare clic su **Next**.

6 Dalla finestra **Refine Case** includere o escludere i tipi differenti di dati dal caso. Le opzioni preconfigurate includono cinque requisiti:

- Inclusione di tutti gli elementi
- Impostazioni ottimali
- Enfasi su e-mail
- Enfasi testo
- Enfasi grafici

7 Fare clic su **Next**.

8 Dalla finestra **Refine Index**, includere ed escludere i tipi differenti di dati dal processo di indicizzazione.

9 Fare clic su **Next**.

Aggiungere prove

1 Fare clic su **Add evidence**. Viene visualizzato il messaggio pop-up **Add Evidence to Case**.

2 Selezionare il tipo di prove da aggiungere al caso: **Acquired Image of Drive**, **Local Drive**, **Contents of a Folder**, o **Individual File** selezionando il pulsante radio. Quindi fare clic su **Continue**.

3 Navigare fino all'immagine, all'unità, alla cartella o al file, selezionare il file e fare clic su **Open**.

Se si è selezionato **Acquired Image of Drive** come tipo di prova, viene visualizzato il messaggio pop-up **Evidence Information**. Inserire le informazioni richieste e fare clic su **OK**.

Se si è selezionata **Local Drive** come tipo di prova

a Viene visualizzato il messaggio pop-up **Select Local Drive**. Selezionare l'unità locale che si desidera aggiungere e quindi selezionare **Logical Analysis** o **Physical Analysis**. Fare clic su **OK**.

b Nella finestra **Evidence Information**, inserire le informazioni richieste quindi fare clic su **OK**.

Se si sono selezionati **Contents of a Folder o Individual File**, selezionare la cartella o il file che si desidera aggiungere al caso, quindi fare clic su **Apri**.

4 Fare clic su **Next**.

5 Nella finestra **New Case Setup is Now Complete**, rivedere le selezioni. Quindi fare clic su **Finish**.

Ingerisci con FTK 3 Lab Edition

Creare un'immagine del dispositivo di storage di destinazione

Consultare "Creare un'immagine del dispositivo di storage di destinazione" a pagina 57.

Creare un caso

1. Fare clic su **Case**→ **New**. Viene visualizzata **New Case Options**.
2. Inserire il nome del caso e le eventuali informazioni di riferimento o descrizioni richieste dalla vostra agenzia.
3. Sfogliare fino alla Directory della cartella del caso e selezionare il Responsabile elaborazione dal menu a discesa.

N.B.: se non si sa dove siano la Directory della cartella del caso e il Responsabile del elaborazione, consultare l'amministratore di sistema.

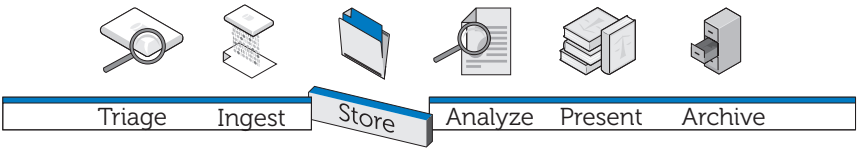
4. Fare clic su **Detailed Options** per rifinire i dati che si desidera includere nel caso. Consultare la *Guida dell'utente sull'accesso ai dati di FTK* 3 per maggiori informazioni sulla restrizione dei dati del caso. Consultare "Documentazione e risorse correlate" a pagina 16.
5. Fare clic su **OK**. Viene visualizzata la finestra **Manage Evidence**.

Aggiungere prove ad un caso

1. Nella finestra **Manage Evidence**, fare clic su **Add**. Quindi fare clic sul pulsante radio affianco al tipo di prova che si desidera aggiungere: **Acquired Image(s)**, **All Images in Directory**, **Contents of a Directory**, **Individual File(s)**, **Physical Drive**, o **Logical Drive**. Quindi fare clic su **OK**.
2. Navigare fino alla directory **Evidence** e selezionare il file delle prove. Quindi fare clic su **Open**.
3. Scegliere un fuso orario (necessario).
4. Fare clic su **OK**. Viene visualizzata la finestra **Data Processing Status**.
5. Quando **Process State** cambia in **Finished**, fare clic su **Close**. La prova viene ora visualizzata nel caso all'interno dell'interfaccia del software.

4

Memorizza



L'approccio tradizionale allo storage delle prove digitali inizia con inquirenti che operano in modo indipendente su singole workstation in una configurazione su silos multipli. Il file delle prove viene memorizzato, in modo più o meno insicuro, sulla workstation o trasferito da un server di storage alla workstation su base giornaliera, appesantendo così la rete con il trasferimento continuo di file molto grandi. La struttura non riesce a sfruttare la velocità di elaborazione distribuita, le economie di scala e i sostanziali risparmi sui costi che l'architettura di elaborazione e storage multi-tier di classe enterprise offre. Inoltre, in questa configurazione, è difficile nella migliore delle ipotesi condividere in modo efficiente i dati o collaborare con team interni ed esterni, per assicurare backup costanti e affidabili dei dati riguardanti le prove, per eseguire l'auditing delle modifiche dei file e, soprattutto, per garantire l'integrità e la sicurezza dei file.

Efficienza

La soluzione Dell Digital Forensics è in grado di adattarsi a molteplici configurazioni IT. Quanto più la configurazione si avvicina in funzionalità ad una vera e propria impresa, costituita da workstation, da server di elaborazione dedicati in grado di eseguire un'elaborazione distribuita, da un'infrastruttura di rete basata sulla comunicazione in parallelo piuttosto che seriale e da storage, maggiore sarà il guadagno in termini di efficienza. Si verifica un traffico di rete minore ma più veloce perché i processori distribuiti si occupano del grosso del lavoro, la rete trasferisce solo i risultati di quel lavoro, piuttosto che il file delle prove veri e propri.

Quando i file delle prove vengono mantenuti sul server anziché sulla workstation, l'analista è libero di utilizzare la workstation per avviare e monitorare lavori *multipli* piuttosto che essere limitato nel tentativo di elaborare un unico lavoro. Inoltre, le analisi possono essere completate più rapidamente, perché molti analisti e specialisti, così come gli esperti di lingue straniere, possono lavorare sullo stesso file ***.E01** contemporaneamente da diverse workstation.

Il lavoro può essere valutato in base alle difficoltà e assegnato ad analisti con diverso grado di esperienza. Un analista junior può farsi carico dei compiti che richiedono più tempo di creazione di grafici da un file ***.E01**, mentre l'analista più esperto senior può spendere meglio il suo tempo eseguendo revisioni più complicate e analisi di quei file grafici.

Scalabilità

Sul back-end, i componenti dei datacenter della soluzione offerta sono modulari e sono progettati con inglobato il concetto di scalabilità. Poiché il datacenter gestisce il carico di lavoro, le workstation non devono essere caricate con memoria e potenza di calcolo. In realtà, terminali molto poco costosi e leggeri possono essere utilizzati per accedere ai file delle prove richiesti e anche al software di analisi memorizzato all'interno del datacenter.

Protezione

La tendenza crescente verso l'aggregazione delle informazioni rende i nostri sistemi di storage di dati sempre più vulnerabili. Allo stesso tempo, l'accesso allo storage delle prove dovrebbe essere la zona più rigorosamente controllata di un sistema digitale per la scientifica. Le best practice richiedono l'implementazione di una strategia di tre livelli:

- Accesso fisico rigorosamente regolamentato che limita l'accesso all'hardware su cui risiedono i dati riguardanti le prove
- Un livello di controllo amministrativo che include l'uso di policy di gruppo
- Sicurezza basata sul computer come policy di creazione password

A tal fine, quando si affronta il problema della progettazione del volume e della struttura adeguata alle vostre esigenze (consultare "Ingerisci" a pagina 39), la sicurezza è la primaria considerazione di un'agenzia quando si tratta di storage.

Livello di accesso fisico

I file del server delle prove digitali della scientifica dovrebbero essere alloggiati in modo più sicuro rispetto a qualsiasi altro file nella vostra organizzazione, compresi i file Risorse Umane.

Considerare i seguenti consigli:

- Posizionare i server per gli esami e lo storage dei dati all'interno di uno spazio di laboratorio esami dedicato. In questo modo, tutti i server, i data warehouse, il cablaggio fisico, gli switch e i router sono fisicamente protetti dalle stesse misure di sicurezza che limitano l'accesso al laboratorio.
- Utilizzare protocolli di controllo d'entrata, come impronte digitali o scansioni della retina o l'accesso con smart card.
- Instradare tutto il traffico relativo agli esami attraverso switch di rete dedicati e collegati fisicamente solo ai server e alle workstation impegnate negli esami.

Livello di controllo amministrativo e Active Directory

La configurazione della soluzione verrà eseguita su un sistema operativo Windows, e quindi il resto di questo capitolo discute di Windows e Active Directory Group e le funzionalità di sicurezza dell'utente. Active Directory è creato sulla base della protezione dei gruppi e le relative funzionalità. Un gruppo è una raccolta di utenti o computer all'interno di un dominio. I due tipi fondamentali di gruppi sono *gruppi di distribuzione* (utilizzati per la distribuzione di posta elettronica) e *gruppi di protezione*. La creazione di gruppi di protezione consente di creare e applicare criteri relativi alla protezione, tra cui:

- Accesso a risorse condivise e livello di tale accesso
- Diritti dell'utente inclusi i requisiti di password
- Policy di blocco di account
- Policy di restrizione del software
- Distribuzione di patch di protezione a portatili, desktop e server

Ad esempio, è possibile creare un gruppo contenente workstation amministrative e un secondo gruppo contenente utenti amministrativi. Quindi, è possibile utilizzare Group Policy Objects (GPO) per limitare l'accesso a quelle workstation e a quei membri del gruppo utenti amministrativi. (Consultare "Applicazione di policy di protezione utilizzando i GPO" a pagina 67 per informazioni sulle modalità di lavoro con i GPO).

Livello di protezione basato su computer e Active Directory

Active Directory offre anche Kerberos, un protocollo di protezione di autenticazione di rete che permette ai nodi comunicanti su reti non sicure di provare la propria identità ad un altro in modalità sicura. Consultare "Account utente Active Directory" a pagina 69 per informazioni sugli account utenti in funzione e consultare anche "Supporto Active Directory per le policy di password sicura" a pagina 68 per informazioni sulla creazione di password.

Informazioni aggiuntive sulla protezione e su Digital Forensics

SP 800-41 Rev. 1 set. Linee guida su firewall e policy sui firewall 2009

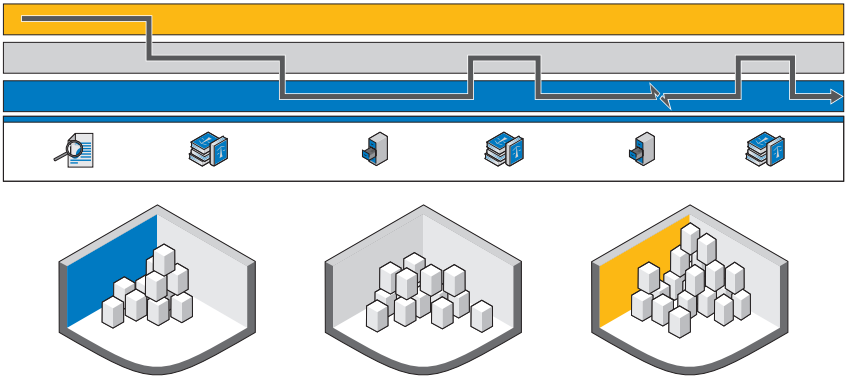
SP 800-46 Rev. 1 giu. Guida su Enterprise Telework e protezione con accesso remoto 2009

SP 800-55 Rev. 1 lug. 2008 Guida sulle misurazione delle prestazioni per la protezione delle informazioni

Storage multi-tier

La soluzione Dell Digital Forensics utilizza strategie di storage multi-tier per affrontare la rapida crescita dei dati e al tempo stesso il controllo dei costi. Un mix di dischi SAS e SATA di capacità e livelli di prestazioni differenti possono essere adattati per abbinare profili di dati, e questo mix può essere rivalutato periodicamente per mantenerne l'ottimizzazione nel tempo. Solitamente, dati mission-critical, come i dati dei casi per i casi attualmente in fase di analisi, vengono memorizzati su unità dalle elevate prestazioni e ad alto costo, mentre i dati meno urgenti, come i file dei casi appena all'inizio dei processi di appello o dei casi chiusi, vengono trasferiti su unità a basso costo e ad elevata capacità.

Figura 4-1. Utilizzo dello storage multi-tier per archiviazione e ripristino



La Figura 4-1 mostra il percorso consigliato per l'archiviazione delle prove digitali dal momento in cui sono raccolte fino alla loro finale conservazione a lungo termine su nastro o cancellazione definitiva.

Corrispondenza dell'archiviazione e del ripristino delle prove con il caso reale

Raccolta delle prove (Analizza). Quando il dispositivo digitale viene inizialmente sequestrato, un laboratorio della scientifica ad alta tecnologia di norma desidera ottenere la prova potenziale dal dispositivo il più rapidamente possibile e avviare il processo di analisi Quanto più velocemente un analista può cercare e indicizzare un file di prova, tanto più rapidamente una decisione può essere presa per far progredire o meno il caso.

Identificazione delle prove (Presenta). Quando la prova è stata potenzialmente trovata durante la fase di analisi, posono essere a questo punto necessarie competenze diverse (lingua, disegni tecnici, contabilità, ecc.). Le prove devono quindi essere classificate per le squadre di visualizzazione. La fase pesante dell'elaborazione è quindi finita e le prove possono quindi risiedere su un tipo di storage a lungo termine più lento e più conveniente.

Attesa del processo (Archivia). Dopo che tutte le possibili prove sono state raccolte e il caso sta procedendo, di solito non c'è bisogno di mantenere i dati del caso e le immagini delle prove nello storage online, dove è possibile accedere istantaneamente. In casi normali, il laboratorio sarà in grado di far fronte al *tempo in giorni di recupero del caso*, che può essere eseguito in modo proattivo, se un evento noto farà scattare il bisogno dei dati del caso. Questo approccio riduce i costi di storage nel laboratorio della scientifica, perché non è necessario conservare tutti i dati in laboratorio, indipendentemente dalla rilevanza attuale, possono essere spostati senza problemi su uno storage più lento.

Processo (Presenta). Nell'eventualità in cui il caso giunga in giudizio, il laboratorio della scientifica desidera avere accesso veloce alle prove e ai dati del caso per rispondere a qualsiasi domanda durante il processo.

Pena detentiva (Archivia). Nel caso di una pena detentiva, la maggior parte dei paesi richiedono che la polizia o il dipartimento di giustizia dipartimento mantengano i file delle prove per un periodo minimo o per la durata della pena detentiva più un ragionevole lasso di tempo per il ricorso o 99 anni. L'obiettivo è quello di inserire i dati su uno storage di lungo e medio termine a basso costo che protegge l'integrità e la riservatezza dei dati.

Ricorso (Presenta). Nell'eventualità di ricorso, i dati del caso e le prove potrebbero dover essere necessari nuovamente per ulteriori analisi o controlli. Questo richiamo dei dati deve avvenire in modo molto puntuale, ma i dati sono molto raramente necessari istantaneamente.

Elimina. Nella maggior parte dei paesi del mondo, gli enti pubblici non sono autorizzati a detenere indefinitamente i dati una volta che essi hanno raggiunto il limite legale di ritenzione. Deve esserci un processo semplice per eliminare tali dati. Questo processo può essere richiesto anche nel caso in cui un verdetto di non colpevolezza sia restituito, e anche i dati devono essere eliminati.

Come impostare Storage Security utilizzando la soluzione Dell Digital Forensics e Active Directory.

Creazione e popolamento di gruppi in Active Directory

I gruppi sono stabiliti attraverso Active Directory Domain Services (Windows Server 2008).

Creazione di un nuovo gruppo (Windows Server 2008)

1. Fare clic su **Start**→ **Administrative Tools**→ **Active Directory Administrative Center**.
2. Nel riquadro di navigazione, fare clic con il tasto destro del mouse sul nodo a cui si desidera aggiungere un nuovo gruppo, fare clic su **New**. Quindi fare clic su **Group**.
3. Inserire il nome del nuovo gruppo.
4. Selezionare l'opzione appropriata in **Group Scope**.
5. Selezionare il **Group Type**.
6. Selezionare **Protect from accidental deletion**.
7. Modificare le sezioni **Managed By**, **Member Of** e **Members**, quindi fare clic su **OK**.

Aggiunta di membri ad un gruppo (Windows Server 2008)

1. Fare clic su **Start**→ **Administrative Tools**→ **Active Directory Administrative Center**.
2. Nel riquadro di navigazione, fare clic sulla cartella in cui risiede il gruppo.
3. Fare clic con il tasto destro del mouse sul gruppo e quindi fare clic su **Properties**.
4. Selezionare **Add** nella scheda **Members**.
5. Inserire il nome dell'utente, del computer o del gruppo che si desidera aggiungere e quindi fare clic su **OK**.

Applicazione di policy di protezione utilizzando i GPO

Dopo aver creato un gruppo, è possibile collettivamente applicare le impostazioni di protezione e altri attributi ai membri di quel gruppo creando e configurando un Group Policy Object (GPO). In questo modo è facile mantenere la protezione per gli utenti e per le risorse digitali al cambiare dell'organizzazione della scientifica.

Creazione e modifica di GPO

Creazione di un nuovo GPO (Windows Server 2008)

In Windows Server 2008, i GPO sono gestiti utilizzando la Console di gestione della policy sui gruppi (GPMC).

1. Per aprire la GPMC, fare clic su **Start**→ **Administrative Tools**→ **Group Policy Management**.
2. Navigare fino alla foresta e al dominio in cui si desidera creare il nuovo oggetto, quindi fare clic su **Group Policy Objects**.
3. Fare clic su **New**.
4. Inserire il nome del nuovo GPO e quindi fare clic su **OK**.

Modifica di un nuovo GPO (Windows Server 2008)

In Windows Server 2008, GPO sono gestiti utilizzando la GPMC.

1. Per aprire la GPMC, fare clic su **Start**→ **Administrative Tools**→ **Group Policy Management**.
2. Navigare fino alla foresta e al dominio in cui risiede il GPO e quindi fare clic su **Group Policy Objects**.
3. Fare clic con il tasto destro del mouse sul GPO.
4. Eseguire le modifiche necessarie alle impostazioni e salvarle.

Supporto Active Directory per le policy di password sicura

Active Directory supporta una varietà di policy di autenticazione, incluse le impostazioni per smart card, password e blocco degli account.

Le password e le altre policy di autenticazione vengono create utilizzando i GPO. Consultare "Applicazione di policy di protezione utilizzando i GPO" a pagina 67 per informazioni sulla creazione e la modifica di un GPO.

Impostazioni per password forti consigliate

I seguenti valori sono suggeriti durante la configurazione delle impostazioni della password:

- Rafforza cronologia password. Il numero di password univoche che devono essere utilizzate prima che una password possa essere riutilizzata. Impostato su 24.
- Validità massima password. Le password devono essere cambiate ogni X giorni. Impostata su 90.
- Validità minima password. Il numero di giorni in cui una password deve essere in vigore prima che possa essere cambiata. Impostata su 1 o 2.
- Lunghezza minima delle password. Impostata da 8 o 12 caratteri.

- La password deve soddisfare i requisiti di complessità. Impostato su **Attivato**. Si applicano le seguenti policy:
  - Le password devono essere lunghe almeno 6 caratteri
  - Le password devono includere caratteri da almeno tre di queste quattro categorie:
    - Caratteri in maiuscolo
    - Caratteri in minuscolo
    - Numeri (da 0 a 9)
    - Simboli
  - Le password non devono contenere tre o più caratteri consecutivi dal nome dell'account o il nome dell'utente

Policy password a grana fine

In Windows Server 2008, Active Directory Domain Services supporta Password Setting Objects (PSO) che si applicano a particolari gruppi di protezione globale o utenti all'interno di un dominio. Un PSO può specificare la lunghezza della password in caratteri, la complessità delle password, la validità minima e massima di una password e altri attributi.

Di conseguenza, è possibile creare PSO multipli che corrispondono alla struttura organizzativa della propria struttura digitale per la scientifica. Ad esempio, è possibile utilizzare PSO per implementare password più lunghe che scadono mensilmente per gli utenti amministrativi e password più brevi che scadono ogni tre mesi per gli analisti.

Account utente Active Directory

Creazione di account utente per gli analisti della scientifica

1. Aprire **Active Directory Users and Computers**:
   a. Fare clic su **Start→ Control Panel**
   b. Fare doppio clic su **Administrative Tools**, e fare doppio clic su **Active Directory Users and Computers**.
2. Nell'albero della console, fare clic con il tasto destro del mouse sulla cartella in cui si desidera aggiungere un account utente.

   Dove?

   Active Directory Users and Computers/*domain node*/*folder*

3 Puntare il cursore su **New**, quindi fare clic su **User**.

4 In **First name**, digitare il nome dell'utente.

5 In **Initials**, digitare le iniziali dell'utente.

6 In **Last name**, digitare il cognome dell'utente.

7 Modificare **Full name** per aggiungere le iniziali o invertire l'ordine del nome e del cognome.

8 In **User logon name**, digitare il nome di accesso dell'utente, fare clic su UPN suffix nell'elenco a discesa e quindi fare clic su **Next**.

Se l'utente utilizza un nome differente per accedere ai computer con Windows 95, Windows 98, o Windows NT, è quindi possibile modificare il nome di accesso utente come viene visualizzato in **User logon name (pre-Windows 2000)** nel nome differente.

9 In **Password** e **Confirm password**, digitare la password dell'utente e quindi selezionare le opzioni password appropriate.

N.B.: per eseguire questa procedura è necessario essere membri dei gruppi Operatori account, Amministratori dominio e Amministratori aziendali in Active Directory; in alternativa, è necessario aver ricevuto delega dall'autorità appropriata. Come best practice per la protezione, considerare l'utilizzo di *Run as* per eseguire questa procedura. Per maggiori informazioni, consultare *Default local groups*, *Default groups* e *Using Run as*.

Creare un Account FTK Service Manager

N.B.: nel corso dell'installazione di FTK, verrà chiesto il nome dell'account utente che si prevede di utilizzare per la gestione delle funzionalità di elaborazione distribuita. Non utilizzare.

Se si utilizza la funzione di elaborazione distribuita di FTK come uno degli strumenti di scientifica digitale, è necessario creare un account FTK Service Manager in Active Directory per gestire l'aggiornamento automatico delle password. Durante il processo di installazione FTK, verrà chiesto di fornire il nome dell'utente che verrà utilizzato per monitorare e gestire la funzione di elaborazione distribuita. Questo account deve essere creato come un servizio in Active Directory, e deve avere privilegi di amministratore (ma non dovrebbe essere l'account Administrator) per fornire la continua collaborazione tra FTK e il server delle prove che la funzionalità di elaborazione distribuita richiede.

1. In Active Directory, aprire **Administrative Tools**, quindi fare clic su **Active Directory Users and Computers**.
2. Nell'albero della console, fare doppio clic sul nodo di dominio.
3. Nel riquadro **Details**, fare clic con il tasto destro del mouse sull'unità organizzativa in cui si desidera aggiungere l'account di servizio. Selezionare **New** e quindi fare clic su **User**.
4. In **Name**, digitare `FTKServMgr` per l'account di servizio e lasciare **Last name** vuoto.
5. Modificare **Full name** come si desidera.
6. In **User logon name**, digitare `FTKServMgr`. L'account di servizio accede con il nome inserito. Dall'elenco a discesa, fare clic su **UPN suffix** accodato al nome di accesso dell'account di servizio (che segue il simbolo @). Fare clic su **Next**.
7. In **Password** e **Confirm password**, digitare una password per l'account di servizio.
8. Selezionare le opzioni password appropriate e quindi fare clic su **Next**.
9. Fare clic su **Finish** per completare la creazione dell'account di servizio.

Creare un account utente non amministrativo

1. Accedere al computer con versione Windows Vista con un account utente amministrativo.
2. Aprire il menu **Start**. Fare clic con il tasto destro del mouse su **Computer** e quindi fare clic su **Manage**.
3. Fare clic sulla freccia vicino a **Local Users and Groups**.
4. Fare clic con il tasto destro del mouse su **Users**, quindi fare clic su **New User**.
5. Digitare il nome dell'utente da qui si sta creando un account. Ad esempio, se si desidera nominare l'utente **webuser1**, dovrete digitare `webuser1` nel campo **Username** e anche nel campo **Full name**.
6. Digitare una password che si ricorderà nei campi **Password** e **Confirm password**.

N.B.: le password distinguono tra maiuscole e minuscole. Le password che si digitano nei campi **Password** e **Confirm Password** devono essere uguali per poter aggiungere l'account utente.

7 Deselezionare la casella di controllo **User must change password at next logon**.

8 Selezionare le caselle di controllo **Password never expires** e **User cannot change password**.

9 Fare clic su **Create**, quindi fare clic su **Close**.

10 Fare clic su **File**, quindi su **Exit**.

Configurazione protezione per file di casi individuali e riguardanti le prove

1 In **Windows Explorer**, navigare fino al file per i quale si desidera stabilire le autorizzazioni file. Fare clic con il tasto destro del mouse e quindi selezionare **Properties**.

2 Fare clic sulla scheda **Security**.

3 Deselezionare la casella di controllo affianco a **Everyone**, se necessario.

4 Aggiungere solo gli utenti che avranno bisogno dell'accesso al file come descritto da policy del luogo di lavoro.

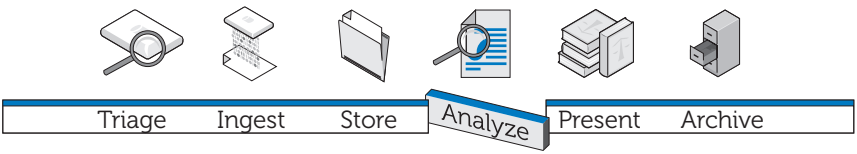
   a Fare clic su **Add**.

   b Nel campo **Enter the object names to select**, inserire i nomi degli utenti appropriati. Quindi fare clic su **OK**.

   c Modificare le **Autorizzazioni** o ogni utente come descritto dalla policy del luogo di lavoro.

5

Analizza



Esistono diversi tipi di analisi che l'investigatore deve essere in grado di condurre sui dati riguardanti le prove, compresa la firma di file e l'analisi hash, l'indicizzazione estesa e le ricerche per parole chiave. Tutte queste analisi richiedono notevole potenza di elaborazione poiché i file delle prove per un singolo caso possono raggiungere dimensioni vicine al range dei terabyte. L'elaborazione di questi file può richiedere decine di ore o addirittura giorni, utilizzando le architetture di datacenter comunemente attive oggi. Gli investigatori che tentano di eseguire questo tipo di analisi su una singola workstation devono tenere conto di questa problematica durante l'elaborazione della pianificazione dei casi, poiché l'analisi e l'indicizzazione di un caso singolo possono utilizzare un numero di risorse hardware superiori a quella a disposizione dall'investigatore. La soluzione Dell Digital Forensics offre vantaggi significativi di elaborazione distribuita che possono cambiare il tutto. A breve daremo uno sguardo all'elaborazione distribuita, ma prima esaminiamo alcuni dei tipi di analisi che l'investigatore della scientifica digitale incontra tipicamente.

Tipi di analisi

Analisi hash

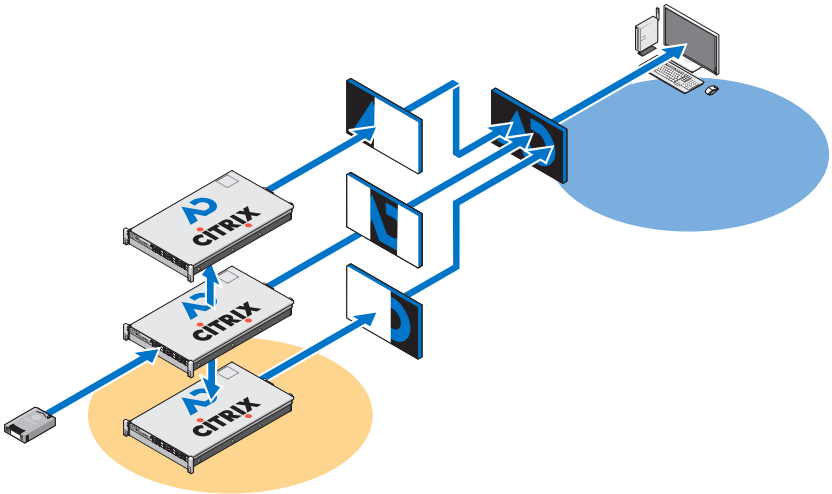
Una funzione hash utilizza algoritmi di crittografia per creare un'impronta digitale di dati. L'hash può essere usato per confrontare un hash dei dati originali con uno dei dati analizzati dalla scientifica, che possono essere accettati in tribunale come prova che i due gruppi di dati sono identici. L'analisi hash confronta i valori hash del file del caso con valori hash noti e memorizzati.

Analisi firma file

Ogni file ha un tipo di file, tipicamente indicato dalle tre o quattro lettere dell'estensione del file. Ad esempio, un file di testo potrebbe avere un'estensione ***.txt** e un file di immagini potrebbe invece avere un'estensione ***.jpg**. Non di rado, queste estensioni di file sono modificate in qualcosa di apparentemente innocuo. Ad esempio, un file immagine potrebbe essere rinominato con un'estensione di file di testo in un tentativo di mascherare il suo contenuto pornografico.

Comunque, ogni file possiede un'intestazione che include un codice del tipo di file differente dall'estensione ma esclusivamente indicativo di un file specifico. Ad esempio, un file ***.bmp**, avrà un codice del tipo di estensione del file ***.bm8**. Quando il codice del tipo di estensione e l'estensione del file differiscono, l'analista della scientifica digitale deve esaminare i dati più attentamente.

Figura 5-1. Elaborazione distribuita



Cos'è l'elaborazione distribuita?

L'elaborazione distribuita si riferisce all'uso di multipli processori, ognuno con le proprie risorse di memoria, applicati individualmente ad una porzione differente di ogni singola attività di elaborazione che utilizzano un sistema di passaggio di messaggi per comunicare tra essi all'interno del gruppo. L'elaborazione distribuita non è l'*elaborazione parallela*, che invece si riferisce ai processori multipli che condividono le stesse risorse di memoria.

Considerate quanto segue ed avrete una vaga idea dei vantaggi della soluzione Dell che utilizza un'installazione di elaborazione distribuita, attraverso un'elaborazione distribuita, che è capace di completare l'analisi di cinque file di 200 GB in sole 3,5 ore, quando l'elaborazione di un singolo file di 200 GB su una workstation standalone potrebbe richiedere circa 7-8 ore.

Lo spostamento dell'elaborazione dei dati relativi alle prove dalla workstation dell'analista al server non è ancora tutto quello che Dell può offrire. La soluzione Dell offre infatti anche la possibilità di utilizzare software di analisi stessa, come FTK e EnCase sul server, consentendo alla workstation di diventare un'interfaccia integrata in grado di eseguire più istanze di diversi pacchetti del software Forensics sotto sistemi contemporaneamente visualizzati senza degrado delle prestazioni del client.

Utilizzo di elaborazione distribuita in FTK 3.1

L'elaborazione distribuita consente di applicare le ulteriori risorse fino a tre ulteriori computer alla volta per l'elaborazione dei casi. Una volta installato e configurato il motore di elaborazione distribuita, è possibile ridurre i tempi di elaborazione dei casi in modo esponenziale.

N.B.: come regola empirica, l'elaborazione distribuita non riduce i tempi di lavorazione a meno che il numero di oggetti da trattare supera 1.000 volte il numero di core presenti all'interno del sistema. Ad esempio, su un sistema con otto core, l'ulteriore distribuzione macchine motore di elaborazione non può ridurre il tempo di elaborazione a meno che le prove contengano più di 8.000 elementi.

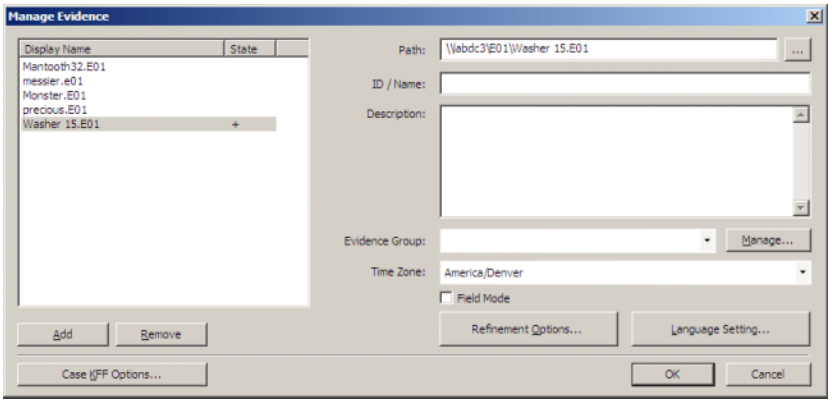
N.B.: per informazioni sull'installazione e la configurazione del modulo di elaborazione distribuita come parte della propria soluzione, fare riferimento alla sezione appropriata della *Guida dell'utente FTK*.

1. Assicurarsi che la cartella del caso sia condivisa prima di tentare di aggiungere ed elaborare prove. Se si stanno seguendo le convenzioni di nominazione dei file consigliate da Dell, la cartella del caso dovrebbe essere posizionata nell'unità del vostro spazio di lavoro, **W:/**. Se non siete sicuri della posizione in cui è posizionata la cartella del caso, contattare l'amministratore di sistema.
2. Inserire il percorso della cartella del caso nella finestra di dialogo **Create New Case** in formato UNC:

   `(\\[computername_or_IP_address]\[pathname]\[filename])`
3. Fare clic su **Detailed Options** e selezionare le opzioni desiderate.
4. Fare clic su **OK** per tornare alla finestra di dialogo **New Case Options**, ed inserire un contrassegno affianco all'opzione **Open the case**. Fare clic su **OK** per creare un nuovo caso e aprirlo.
5. Fare clic su **Add** dopo che un nuovo caso viene aperto e la finestra di dialogo **Manage Evidence** si apre automaticamente. Selezionare il file prove da aggiungere e quindi fare clic su **Open**.
6. Il percorso per le prove viene creato in modo predefinito per lettera di unità. Modificare il percorso in formato UNC modificando la lettera dell'unità nel nome della macchina o dell'indirizzo IP in cui si trova il file delle prove, in base alla seguente sintassi:

   `\\[computername_or_IP_address]\[pathname]\[filename]`
7. Lasciare il resto del percorso come è.
8. Il percorso UNC per le prove è illustrato nella seguente figura:

Figura 5-2. Finestra di dialogo Manage Evidence



9. Fare clic su **OK**.

Verifica installazione

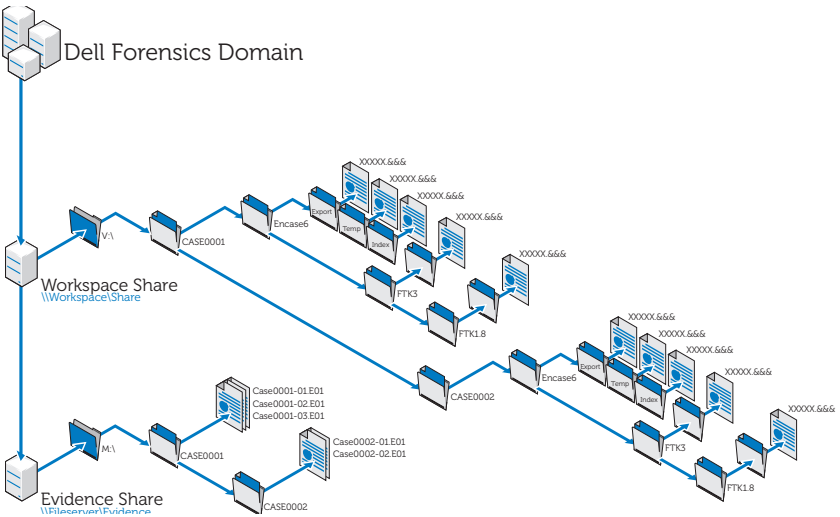
Quando si completa l'installazione, aprire **Task Manager** sul computer remoto e tenerlo aperto mentre si aggiungono prove e iniziare l'elaborazione. Questi passaggi permettono di osservare l'attività di **ProcessingEngine.exe** nella scheda **Processes**.

Il motore di elaborazione distribuita non viene attivato fino a che un caso supera approssimativamente i 30.000 elementi. Quando si attiva, è possibile vedere l'aumento delle percentuali di utilizzo della CPU e della Memoria per **ProcessingEngine.exe** in **Task Manager**.

Identificazione file su rete

Le best practice richiedono che le prove e i file di lavoro siano memorizzati separatamente sulla rete. Dell consiglia di configurare due unità condivise e quindi creare file e sottoflile dei casi da lì come mostrato in Figura 5-3.

Figura 5-3. Struttura file consigliata da Dell



Analisi con FTK

Aprire un caso esistente

Utilizzo del menu file

1. Dall'interno di FTK, selezionare **File**, quindi selezionare **Open Case**.
2. Evidenziare il caso che si desidera aprire per avviare il caso.

N.B.: tutti i file del caso vengono nominati **case.ftk**. Il file **case.ftk** per ogni caso viene archiviato nella cartella del caso di riferimento.

Dalla linea di comando

Nella linea di comando digitare:

```
path_to_ftk_program_file\ftk.exe /OpenCase
target_case_directory
```

Elaborazione prove di un caso

FTK elabora le prove nel momento in cui viene creato un caso o quando vengono aggiunte prove ad un caso esistente. Per istruzioni sulla creazione di un nuovo caso, consultare "Creare un caso" a pagina 60 o fare riferimento alla *Guida dell'utente FTK*. Per istruzioni sull'aggiunta di prove ad un caso esistente, consultare "Aggiungere prove ad un caso" a pagina 60 o fare riferimento alla *Guida dell'utente FTK*. Per ulteriori informazioni, consultare "Documentazione e risorse correlate" a pagina 16.

Analisi con EnCase

Aprire un caso esistente

1. Dal menu file, sezionare **File→ Open**.
2. Sfogliare fino al caso e fare clic su **Open**.

Creare un lavoro di analisi

1. Fare clic sulla scheda **Analysis Jobs** nella finestra di dialogo principale **Source Processor**.
2. Fare clic su **New**. Viene visualizzata la finestra di dialogo **Create Analysis Job/Job Name**.

   Il nome predefinito del lavoro è Job__[yyyy_mm_dd__hh_mm_ss], ad esempio: Job___2009_06_24__03_42_42_PM.

   Un nome di un lavoro non deve contenere spazi all'inizio o alla fine del nome e nessuno dei seguenti caratteri: \ / : * ? " < > |
3. Inserire il nome di un lavoro e fare clic su **Next**. Viene visualizzata la finestra di dialogo **Create Analysis Job/Module Selection**.

   Questa finestra mostra le cartelle del modulo nel riquadro a sinistra e i singoli moduli all'interno di queste cartelle nel riquadro di destra.

   Se un modulo è incluso in un lavoro di analisi, ma non ci sono dati per quel modulo quando quel lavoro viene seguito nei confronti di una raccolta, il modulo viene ignorato. Questa funzione consente di creare lavori di analisi generici per una varietà di set di dati raccolti.
4. Riempire una casella di controllo del modulo.

   È possibile selezionare più di un modulo.

   I moduli di analisi non hanno impostazioni configurabili dall'utente.

   Per selezionare tutti i moduli in un gruppo, riempire una casella di controllo accanto al nome di quel gruppo nel riquadro sinistro.
5. Fare clic su **Finish**.

N.B.: i lavori di analisi potrebbero elencare i moduli non presenti nei lavori raccolti. Tali moduli sono identificati come moduli di legacy di modo che sia possibile analizzare i dati raccolti nelle precedenti versioni del Source Processor utilizzando i moduli che non esistono più.

Eseguire un lavoro di analisi

1. Dalla scheda **Collected Data**, selezionare la prova che si desidera analizzare per prima selezionando il nome del lavoro nel riquadro a sinistra. Quindi, selezionare i file delle prove reali nella tabella a destra.

2. Fare clic su **Run Analysis**. Viene visualizzata la finestra di dialogo **Select Analysis to Run**.
3. Selezionare il lavoro di analisi e quindi fare clic su **Run**. Source Processor esegue l'analisi sulle prove selezionate. Quando l'analisi è completata, viene visualizzato il browser dei dati.

Esecuzione dell'analisi della firma

1. Fare clic su **Search**.
2. Selezionare la casella **Verify file signatures** nell'area **Additional Options** in basso a destra e quindi fare clic su **Start**. La routine dell'analisi della firma viene eseguita in background. Al completamento, viene visualizzata una finestra di dialogo di ricerca completata. La finestra di dialogo presenta lo stato, i tempi e i dati di file relativi alla ricerca.

Gli stessi dati sono visualizzabili nella console.

Visualizzazione dei risultati dell'analisi della firma

1. Fare clic su **Set Include** nel pannello **Tree** per visualizzare tutti i file del caso.

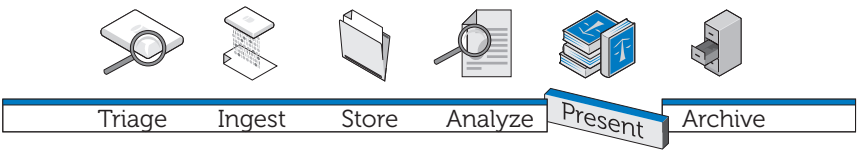
   A questo punto, **Set Include** seleziona tutto ciò che si presenta nel file delle prove.
2. Organizzare le colonne nel riquadro **Table** così che le colonne **Name**, **File Ext** e **Signature** siano una affianco all'altra.
3. Ordinare le colonne con **Signature** al primo livello, **File Ext** al secondo livello e **Name** al terzo livello.

   Scorrere verso l'alto o il basso per vedere tutte le firme.
4. Fare clic su **Set-Include** nella selezione **Entries** nel riquadro **Tree**.

   Viene dunque visualizzato un elenco dei file dei casi con le relative firme e altri dati nel riquadro **Table**.
5. Ordinare i dati come lo si desidera.

6

Presenta



La creazione di report sui risultati delle analisi è parte integrante della Soluzione Dell Digital Forensics ed è gestita primariamente tramite il software Forensics che si sta utilizzando come parte della soluzione.

Come creare report con la soluzione Dell Digital Forensics

Creare ed esportare report con EnCase 6

1. Selezionare gli elementi su cui eseguire un report, file, segnalibri, risultati di ricerca o altri dati.
2. Selezionare il tipo di report che si desidera utilizzando le schede nel riquadro **Tree**.
3. Dalla scheda **Table** nel riquadro **Table**, abilitare gli elementi che si desidera mostrare nel report.
4. Dalla scheda **Table**, passare alla scheda **Report**.
5. Modificare il report come desiderato.
6. Esportare il report in un formato visualizzabile al di fuori di EnCase.
   a. Fare clic con il tasto destro del mouse nel report e fare clic su **Export** dal menu a discesa. Viene visualizzata la finestra di dialogo **Export Report**.
   b. Fare clic su pulsante radio appropriato per selezionare il formato finale che si desidera utilizzare (TEXT, RTF o HTML).

c Raggiungere o navigare verso il percorso di produzione.

d Se lo si desidera, selezionare **Burn to Disc** per abilitare la casella **Destination Folder**, quindi fare clic con il tasto destro del mouse su **Archive Files** per creare una nuova cartella e salvare un file **.iso** sul disco.

e Fare clic su **OK**.

Report con FTK

1 Fare clic su **File→ Report** per avviare **Report Wizard**.

2 Inserire le informazioni di base richieste dalla procedura.

3 Selezionare le proprietà per i segnalibri.

4 Determinare se e come si desidera visualizzare i grafici relativi al caso nel report.

5 Determinare se si desidera includere una sezione che elenchi i percorsi e le proprietà dei file nelle categorie selezionate.

6 Aggiungere le sezioni **Registry Viewer** se lo si desidera.

Visualizzare il report al di fuori di FTK

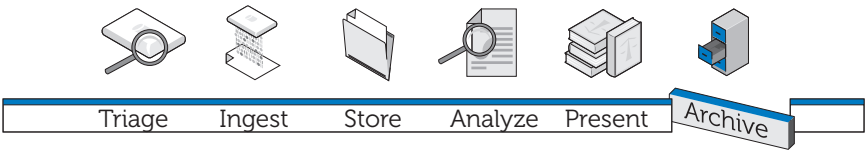
1 Cercare il file del report.

2 Fare clic sul file del report e in seguito:

- Fare clic su **index.htm** per aprire un documento HTML in un browser Web.
- Fare clic su [*report*]**.pdf** per aprire il report in un visualizzatore PDF.

7

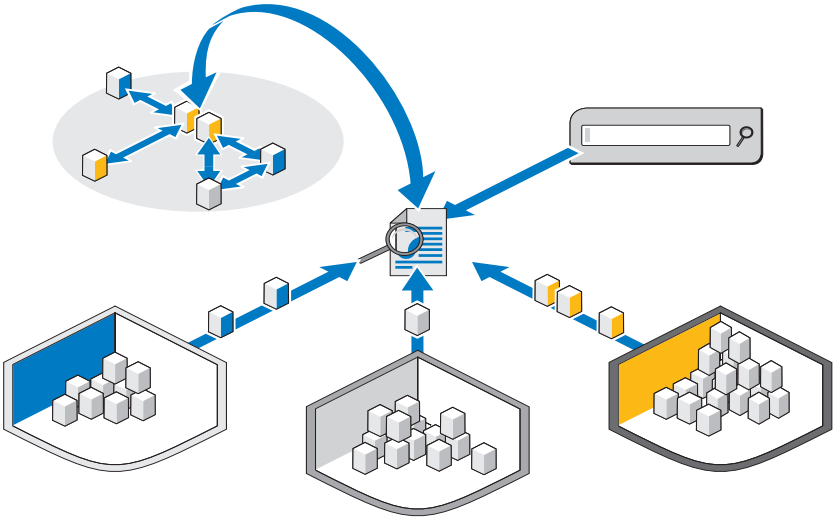
Archivia



Nessuna soluzione digitale per la scientifica è completa senza un componente di archiviazione e recupero scalabile, sicuro e completo. La soluzione Dell Digital Forensics offre questo e altro ancora. Nella struttura della soluzione Dell, abbiamo cercato di creare una semplice interfaccia capace di funzionare con tutte le applicazioni per la scientifica per controllare il ciclo di vita delle prove e dei file dei casi. Poiché risulta difficile prevedere quando i dati potrebbero essere necessari in futuro o per quanto tempo può durare l'indagine, abbiamo creato una soluzione flessibile che richiede il singolo analista della scientifica per determinare i file che ricorderà e archivierà. Questa soluzione utilizza un approccio graduale allo storage in base alle vostre esigenze. Un mix di hardware SATA e SAS e archiviazione gestita dall'utente con il software di archiviazione on demand di NTP.

La soluzione di Dell è costituita da componenti modulari che forniscono un ambiente scalabile che può essere ampliato per soddisfare la crescente domanda di requisiti di elaborazione e storage. L'infrastruttura di backup, ripristino e archiviazione (BURA) formalizzata dalla soluzione aiuta ad ottimizzare la cooperazione tra le agenzie e le forze, oltre i confini. Libera dagli oneri amministrativi automatizzando gran parte dell'attività di backup dei dati, fornisce la coerenza tra laboratori interagenzia e riduce i rischi per la catena di custodia digitale.

Figura 7-1. Capacità di ricerca tra supporti e tra casi della soluzione Dell



Un componente molto potente di ricerca facoltativo consente la correlazione di informazioni tra insiemi di dati ingeriti. Questo componente offre la possibilità di condurre ricerche su Internet, come su l'intero archivio di dati sui casi, su contenuti sia attivi che online, così come sul materiale archiviato dai casi precedenti.

Soluzione di archiviazione con un singolo clic del client

Utilizzando gli strumenti della soluzione di Dell Digital Forensics di archiviazione e recupero, un analista può archiviare o richiamare sia singoli file che intere strutture di directory facendo semplicemente clic con il tasto destro del mouse. Sono stati aggiuntivi ulteriori comandi tramite il tasto destro del mouse al software di archiviazione on demand di NTP in modo che l'utente deve semplicemente selezionare e archiviare, o selezionare e ripristinare i dati. Quando un file viene selezionato per l'archiviazione, viene visualizzata una finestra supplementare che richiede all'utente di confermare l'azione. Se la si conferma, la soluzione eseguirà un processo in background per spostare quel file su un dispositivo a nastro o su un dispositivo di archiviazione near-line. Questo processo avviene completamente senza interruzioni dell'attività in background, senza degrado di alcuna delle prestazioni della workstation dell'utente.

Quando il processo in background viene completato, l'icona del file attribuito a quel file diventa di color grigio ad indicare in modo chiaro per l'utente che il file è stato archiviato. La cartella e la struttura dei file sono ancora visibili in modo che l'utente possa facilmente trovare il file di nuovo in futuro ai fini di ripristino. Per ripristinare un file, l'utente deve semplicemente navigare attraverso la struttura della cartella originale, individuare la cartella o il file che desidera ripristinare, fare clic con il tasto destro sul file o sulla cartella, quindi selezionare l'opzione di ripristino.

Dell consiglia che tutti i file e i file dei casi siano situati su un dispositivo NAS centrale scalabile che permetta un punto di storage centrale espandibile, consentendo una facile collaborazione tra gli analisti. Questa raccomandazione permette anche un singolo punto di controllo per motivi di catena di custodia. Quando un file viene selezionato per l'archiviazione, viene spostato nella finestra successiva disponibile del sistema di elaborazione dallo storage primario ad un'opzione secondaria (nastro o near-line).

I tempi di archiviazione e recupero possono variare notevolmente a seconda del traffico corrente da e per lo storage NAS centralizzato, dei file correnti in via di archiviazione e dal tipo di supporto che comprende l'opzione di storage secondario. Per esempio, SATA near-line offrirà tassi di completamento molto più veloci della soluzione su nastro. Tutti i file possono essere crittografati su nastro per una maggiore sicurezza quando raggiungono la fase di archiviazione a lungo termine della soluzione, che può richiedere ulteriori licenze.

Consigli per il backup Dell

Backup di prove e file dei casi

Un laboratorio della scientifica presenta tre tipi di file core:

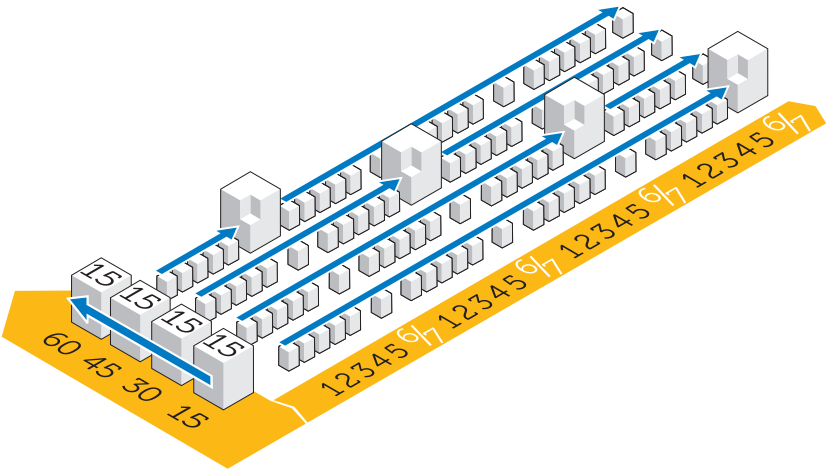
- File immagini: questi sono immagini basate sui ritrovamenti effettuati sul dispositivo sospetto. Una volta ingeriti, non cambiano e occorre eseguirne il backup solo una volta (possibili estensioni: **E01**, **DD**, ecc). I file di prova tendono a trovarsi a basso contenuto di quantità, ma di dimensioni molto grandi.
- File dei casi: questi sono i file dati e gli indici che sono il risultato delle analisi; che potrebbe dover essere esportati al di fuori dell'applicazione per la scientifica. I file modificati di frequente, se il caso è attualmente live, possono contenere più tipi di estensione, che richiedono il backup su base giornaliera. I file dei casi tendono ad essere numerosi a livello di quantità, ma di solito sono di dimensioni molto ridotte.

- Database: questo tipo di file è usato solo in FTK 3 (al momento), ma contiene tutti i collegamenti tra i file di dati e i file di prova, così come tutti i segnalibri e le note dell'investigazione. Il backup dei file database deve essere eseguito su base giornaliera.

La Figura 7-2 mostra le best practice consigliate per eseguire il backup di un laboratorio della scientifica digitale. Poiché molti laboratori della scientifica hanno più di 50 TB di storage, potrebbe non essere possibile portare a termine un backup completo in una finestra weekend di backup standard. Per garantire che in caso di un disastro i dati possono essere ripristinati con il punto di ripristino minimo possibile, il backup è diviso in sezioni uguali ed è gestito nell'arco di un mese.

Questo processo richiede che la dimensione massima di backup sia limitata a 15 TB per ogni backup completo. Ogni LUN poi prende aggiornamenti incrementali per il resto del ciclo di backup fino a che un backup completo risulti necessario.

Figura 7-2. Piano di backup con best practice



Altro host vs. Rete

A causa della dimensione dei dati che devono essere spostati su nastro per scopi di disaster recovery, nella maggior parte dei laboratori della scientifica, lo storage delle LUN viene diviso in LUN da 15 TB. Questo requisito consente gestione e backup più semplici e riduce anche gli errori di cluster del File System nel tempo in caso di guasto.

Possono essere eseguiti due tipi di backup, attraverso la rete o come altro host.

- In una configurazione su rete, tutti i dati vengono trasmessi attraverso la rete al server di backup utilizzando un agente di backup residente sul server.
- In una soluzione di backup su altro host, alcuni dei server con gli archivi di file più grandi non eseguono il backup dei propri dati attraverso la rete. Al contrario, lo storage array cattura una snapshot della LUN e poi monta la copia direttamente sul server di backup. Questo processo aumenta la velocità complessiva di backup poiché nessun file di backup viene trasmesso attraverso la normale rete per causare ulteriori problemi di conflitto di rete.

In molti laboratori della scientifica odierni, i backup vengono effettuati su reti da più di 10 GB.

La figura seguente mostra gli agent necessari per singolo server per facilitare il backup:

Figura 7-3. Agent di backup

Name	Qty	Type	Application	OF	AD	OA	SA	BE	NBU	EV	Cluster	MI	SS
	1	M610	SQL Server	X			X				No	X	X
	1	M610	NTP file auditor	X							No		X
	2	M610	Active Directory	X	X						No	X	X
	4	M610	Siloed Citrix	X							No		X
	7	M610	FTK & Oracle	X		X					No	X	X
	2	M910	File Server	X							Yes	X	X
	2	M610	Encase & FTK1.8	X							No		X
	1	M610	Enterprise Vault	X						20 Users	No		X
	2	R710	Backup Exec	X				X			No	X	X
	0	n/a	Web Server	X							No		X

OF Agent Open File

AD Active Directory

OA Agent Oracle (agent database generico richiesto su Backup Exec Symantec)

SA Agent SQL (agent database generico richiesto su Backup Exec)

NBU Server Net Backup

BE Server Backup Exec

EV Licenza di backup Symantec Enterprise Vault

MI Backup mensile completo, giornaliero incrementale

SS Stato di sistema verificato una volta al mese

N.B.: data la crescita dei dati nel tempo, potrebbe essere richiesta una soluzione su altro host.

Come creare report con la soluzione Dell Digital Forensics

Archiviazione on demand

ODDM del software NTP il movimento dei dato con tasto destro del mouse (RCDM) di (RCDM) lavorano in collaborazione con Enterprise Vault per ridurre la necessità di scansioni dell'intero File System, come per l'archiviazione tradizionale, mediante l'esecuzione di archiviazione on *demand*. I costi di storage vengono così ridotti e la qualità dell'archiviazione viene invece migliorata.

A seconda della fase del ciclo di vita dei dati, come descritto in "Corrispondenza dell'archiviazione e del ripristino delle prove con il caso reale" a pagina 65, l'analista può scegliere di archiviare i dati in storage di lungo periodo, o conservare i dati per un accesso ed elaborazione immediati.

Inoltre, ODDM del software NTP può essere utilizzato per archiviare automaticamente i dati che devono essere conservati per motivi legali.

Requisiti

ODDM del software NTP richiede Microsoft IIS, Microsoft .NET Framework, SQL e Enterprise Vault. ODDM del software NTP e Enterprise Vault devono essere installati sullo stesso server. Installazioni di grandi dimensioni sono in grado di mantenere il database SQL su un server dedicato.

Installazione

Per istruzioni di installazione dettagliate per ODDM del software NTP e RCDM del software NTP, consultare la *Guida di installazione e configurazione di Dell Digital Forensics*. Per ulteriori informazioni, consultare "Documentazione e risorse correlate" a pagina 16.

Archivia: con ODDM del software NTP

Archiviazione gestita dall'utente

1 Quando l'analista archivia file di dati, QFS del software NTP avvisa l'utente che potrebbe essere necessario archiviare i file.

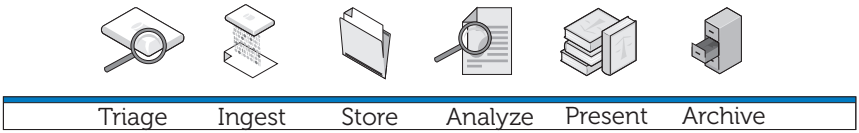
2 L'analista seleziona i file da archiviare con Storage Investigator del software, quindi fa clic su **Archivia**. Tuttavia, se il componente aggiuntivo RCDM di NTP non è installato, fa clic con il tasto destro del mouse sui file.

Quando i file vengono selezionati, Storage Investigator del software NTP notifica ODMM del software NTP, che a sua volta attiva Enterprise Vault.

La richiesta di archiviazione viene aggiunta alla coda di archiviazione.

8

Risoluzione dei problemi



Suggerimento sulla risoluzione dei problemi

- Assicurarsi che tutti i client e i server possano visualizzarsi a vicenda e che siano in grado di effettuare il ping tramite il nome NetBIOS e l'indirizzo IP.
- Assicurarsi che i firewall permettano il traffico.
- Riavviare i server e i client per assicurarsi che tutte le modifiche di installazione e configurazione siano state riconosciute dal sistema.

Problematiche specifiche del software Forensics

EnCase: EnCase si avvia in modalità Acquisizione

Questo problema indica che EnCase non è dotato di licenza.

1. All'interno di EnCase selezionare **Tools→ Options** e assicurarsi che **User Key Path**, **Server Key Path** e **Server Address** siano riempiti (questi campi dovrebbero condurre alla posizione delle chiavi della licenza).
2. Verificare il firewall sul client e sul server della licenza EnCase per assicurarsi che la porta 4445 sia aperta.
3. Assicurarsi che il client possa effettuare il ping del server della licenza EnCase.

FTK Lab: il browser avviato dal client non riesce a visualizzare l'Interfaccia Utente

1. Assicurarsi che il client abbia MS Silverlight installato.
2. Assicurarsi che i servizi Oracle siano stati avviati sul server che fa da host al database Oracle.

FTK 1.8: messaggio di limite\versione di prova 5000 oggetti

Se si riceve questo messaggio significa che FTK non ha licenza. Assicurarsi che il server della licenza di rete sia in funzione e presenti le licenze FTK 1.8:

1. Aprire una finestra browser sul server che fa da host al servizio di licenza di rete e inserire **http://localhost:5555** nella barra dell'indirizzo.
2. Vedere se le licenze siano presenti. Se non lo sono, è necessario installarle.

FTK 1.8: impossibile accedere, l'errore Access Temp File viene visualizzato all'avvio

Consentire all'utente di avviare l'applicazione (o la sessione Citrix) per avere accesso al disco rigido del server O eseguire l'applicazione come amministratore.

Problematiche Citrix

Le applicazioni Citrix: non si avviano

1. Assicurarsi che tutti i servizi (in particolare MFCOM e IMA) siano avviati sui server che fanno da host a XenApp.
2. Assicurarsi che il client possa visualizzare i server XenApp ed effettuarne il ping.
3. Verificare i firewall sui client e sui server XenApp per assicurarsi che le porte XenApp siano aperte.
4. Verificare il server della licenza Citrix per assicurarsi che il servizio di licenza di rete abbia una licenza da emettere. Il server di licenza Citrix è solitamente installato su uno dei server Citrix XenApp, accessibili da **Start→ Programmi→ Citrix→ Management Consoles→ Citrix Licensing**.

5 Aprire **Citrix Management Console** (**Start→ Programmi→ Citrix→ Management Consoles→ Citrix Delivery Services console**). Quindi eseguire un rilevamento per assicurarsi che tutti i server XenApp siano presenti nel farm.

6 Assicurarsi che l'applicazione sia stata pubblicata su un server XenApp valido (incluso nel farm).

7 Vedere nella **Citrix Delivery Services Console** per assicurarsi che l'utente che sta avviando le applicazioni sia in un Gruppo che può avviare l'applicazione.

8 Per le applicazioni inviate, assicurarsi che il Controllo dell'account utente (UAC) sia disattivato sul server.

Applicazioni Citrix bloccate o arrestate

Quando gli utenti non effettuano in modo appropriato la disconnessione dalle sessioni di Citrix, le sessioni orfane iniziano a rallentare e potrebbero infine causare il blocco o l'arresto del server. Dunque, è estremamente importante che gli utenti seguano le best practice per effettuare la disconnessione in modo appropriato per ogni sessione (**Start→ Logoff→ Ok**) e non semplicemente che facciamo clic sulla *x* nella casella nell'angolo in alto a destra della finestra della sessione.

Ad ogni modo, è possibile riscontrare nuovamente questa problematica e ci sono due metodi per risolverla:

1 Effettuare la disconnessione dell'utente in modo manuale.

   a Aprire una sessione come amministratore Citrix.

   b Rivedere l'elenco delle sessioni aperte e chiudere in modo manuale ognuna di esse.

2 Riavviare il server.

Indice analitico

A

Acquisizione Live
  vs. Acquisizione standard, 20

Acquisizione standard
  vs. Acquisizione Live, 20

Analisi firma file, 74

Analisi hash, 73

Analizza, 9-10, 65, 73
  EnCase, 78
  tipi di analisi, 73

Archivia, 9, 11, 66, 89
  con NTP Software ODDM, 89
  con un singolo clic del client, 84
  e tempi di richiamata, 85

Archiviazione on demand, 89
  installazione, 89
  ODDM, 89
  RCDM, 89
  requisiti, 89

B

Backup, 85
  agent, 88
  best practice, 86
  rete, 87
  su altro host, 87
  su altro host vs. rete, 86

C

Collector
  pulizia, 23
  Registra, 21
  utilizzo, 34

Componenti della soluzione, 12

Computer ruggedi
  come accenderlo, 20

Configurazione di rete, 48
  convenzioni nominazione gruppo NIC, 49
  convenzioni nominazione server, 48
  mapping lettera unità, 49
  struttura file, 50
  struttura indirizzo IP, 48

D

Disco archivio
  pulizia, 23
  registra, 21

E

Elaborazione distribuita
  con FTK 3.1, 75
  confronto con l'elaborazione parallela, 75
  definizione, 75

EnCase
abilitato per datacenter, 39
analisi, 78
come aprire un caso già esistente, 78
come creare un lavoro di analisi, 79
come effettuare un'analisi della firma, 80
come eseguire un lavoro di analisi, 79
creare ed esportare report, 81
risoluzione dei problemi, 91

F

FTK
1.8 e 3.0 abilitato per datacenter, ingerisci, 56
1.8, abilitato per datacenter, 42
3, abilitato per datacenter, 43
3, Lab Edition, 46
3.0 Lab Edition, ingerisci, 59
visualizzazione report, 82

I

Ingerisci, 9, 39, 51
con EnCase, 53
con FTK, 56
con SPEKTOR, 51
definizione, 10

M

Memorizza, 9-10, 61

N

NTP Software ODDM, 89
NTP Software RCDM, 89

P

Presenta, 9, 11, 65-66, 81
Profilo collector
configurazione, 23

R

Risoluzione dei problemi, 91
Citrix, 92
EnCase, 91
FTK 1.8, 92
FTK Lab, 92
software Forensics, 91
suggerimenti generali, 91

S

Soluzione della soluzione
nel campo, 12
nel datacebter, 13

SPEKTOR
configurare un collectore per acquisizione, 24
ingerisci, 51
modulo imager opzionale, 10
registrare un collector o un disco archivio, 23
registrare un disco collector o archivio, 21
revisioni report, 36
utilizzo contro target, 33
Storage multi-tier, 64

T

Tableau Write-Blocker, 54
connessione a IDE HD, 55
connessione a SATA HD, 55

V

Valutazione, 9, 17, 83
come eseguirla, 20
definizione, 17
revizione file raccolti, 36